

IPL-C

Routeur cellulaire 4G 3G - serveur RAS - firewall

NOTICE D'UTILISATION
Document référence : 9021509-01

SOMMAIRE

PRESENTATION

INSTALLATION

MISE EN SERVICE

SOMMAIRE

… MISE EN SERVICE

…MISE EN SERVICE

SOMMAIRE

… MISE EN SERVICE

MAINTENANCE

1 Déclaration de conformité

Identification : Routeur cellulaire & firewall & serveur RAS

Référence : IPL-C

Au nom de la société ETIC Telecom, Gilles Bénas agissant en tant que directeur de la qualité, déclare que le produit ci-dessus est conforme à la directive R&TTE Directive (1999/5/EC).

Le produit routeur est en particulier conforme aux normes suivantes :

Compatibilité :	EN 55022 EN 50024 EN 300386-2 FCC Part 15
Sécurité :	EN 60950 UL (IEC950)
Substance dangereuses :	2002/95/CE (RoHS)

Date : 4 Février 2015

Gilles Bénas
Responsable de la qualité

2 Identification des produits

La présente notice décrit la mise en service et l'utilisation des produits suivants :

Routeur cellulaire sans interface Wifi					
IPL-C-	**400-XY**	**220-XY**	**230-XY**	**260-XY**	**261-XY**
Routeur cellulaire 4G-3G-GPRS-EDGE (selon code XY) Routeur 3G, GPRS-EDGE : XY = HG Routeur 4G, 3G, GPRS-EDGE : XY =LE	•	•	•	•	•
Firewall SPI	•	•	•	•	•
Serveur RAS 25 utilisateurs	•	•	•	•	•
VPN IPSEC & SSL	•	•	•	•	•
Passerelle série (Raw TCP et UDP, Telnet, Modbus, Unitelway)	-	•	•		•
Ethernet 10 / 100 BT	4	2	2	2	2
RS232	-	1	2	-	-
RS485	-	1	-	-	-
RS422 isolée	-	-	-	1	-
RS485 isolée	-	-	-	-	1
USB	1	1	1	1	1
Routeur IP	•	•	•	•	•
NAT	•	•	•	•	•
Redirection de port (port forwarding)	•	•	•	•	•
SNMP	•	•	•	•	•
DNS	•	•	•	•	•
DHCP client ou serveur sur l'interface LAN	•	•	•	•	•
Entrée TOR pour email d'alarmes	1	1	1	1	1
Configuration HTTPS / HTML / SSH	•	•	•	•	•
IO Viewer : Module optionnel de visualisation d'entrées sorties modbus	•	•	•	•	•

Routeur cellulaire avec interface Wifi					
IPL-CW-	400-XY	220-XY	230-XY	260-XY	261-XY
Routeur cellulaire 4G-3G-GPRS-EDGE (selon code XY) Routeur 3G, GPRS-EDGE : XY = HG Routeur 4G, 3G, GPRS-EDGE : XY =LE	•	•	•	•	•
Interface WiFi 2,4 GHz et 5 GHz	•	•	•	•	•
Firewall SPI	•	•	•	•	•
Serveur RAS 25 utilisateurs	•	•	•	•	•
VPN IPSEC & SSL	•	•	•	•	•
Passerelle série (Raw TCP et UDP, Telnet, Modbus, Unitelway)	-	•	•		•
Ethernet 10 / 100 BT	4	2	2	2	2
RS232	-	1	2	-	-
RS485	-	1	-	-	-
RS422 isolée	-	-	-	1	-
RS485 isolée	-	-	-	-	1
USB	1	1	1	1	1
Routeur IP	•	•	•	•	•
NAT	•	•	•	•	•
Redirection de port (port forwarding)	•	•	•	•	•
SNMP	•	•	•	•	•
DNS	•	•	•	•	•
DHCP client ou serveur sur l'interface LAN	•	•	•	•	•
Entrée TOR pour email d'alarmes	1	1	1	1	1
Configuration HTTPS / HTML /SSH	•	•	•	•	•
IO Viewer : Module optionnel de visualisation d'entrées sorties modbus	•	•	•	•	•

Service de connexion M2Me_	

Service de connexion M2Me_Connect IPL_M2Me
Composants recouverts de vernis hydrofuge IPLC_PCBD

3 Présentation

Le routeur IPL-C est à la fois un routeur cellulaire 4G-3G-GPRS-EDGE, un firewall et un serveur d'accès distant (RAS).

Il permet de connecter des machines industrielles sur l'internet avec un haut niveau de sécurité et confidentialité pour réaliser des systèmes de télé-contrôle (SCADA).

Il offre les fonctions suivantes :

4G-3G-GPRS-EDGE à double carte SIM

Routeur IP : Table de routage, RIP, SNMP, VRRP.

Client et serveur VPN IPSec ou OpenVPN.

Service d'accès distant (RAS) pour les opérations de télémaintenance ou télé-exploitation par PC tablette ou smartphone.

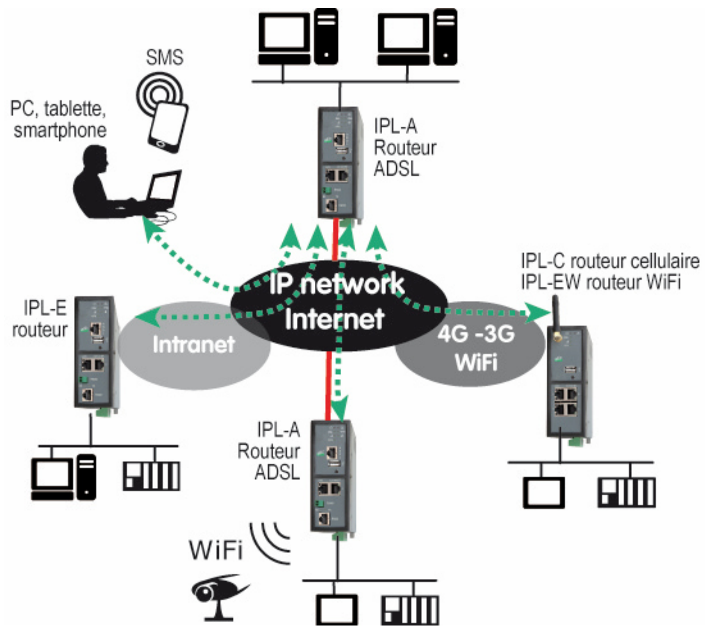
Firewall

Interfaces série et WiFi optionnels

3.1 Applications

Système de télé-contrôle
Le routeur IPL-C permet d'interconnecter des équipements industriels au moyen de l'Internet avec un niveau élevé de sécurité et confidentialité.

Pour la télémaintenance ou la télé-exploitation, un opérateur peut se connecter à distance à l'un quelconque des équipements du système au moyen d'un PC, d'une tablette ou d'un smartphone.
Ses droits peuvent être limités en fonction de son identité.



3.2 Fonctions du routeur

Routage
Le routeur IPL-C offre une large gamme de solutions de routage qui peuvent être mises en œuvre selon le besoin pour assurer la communication entre les machines de chaque réseau à connecter :
Connexions distantes décrivant les réseaux directement accessibles,
Routes statiques, pour atteindre des réseaux nichés,
Translation d'adresse (NAT, DNAT, port forwarding),
Protocole automatique d'échange de table de routage (RIP),
Gestion de nom de domaine DNS et DynDNS.

VPN IPSec et OpenVPN pour la sécurité
Le router IPL-C permet d'établir des tunnels VPN de type IPSec ou OpenVPN.
Il peut se comporter en client ou en serveur VPN.

La connexion VPN garantit un niveau élevé de performance et de sécurité

Transparence : Etabli entre deux routeurs, le VPN assure l'interconnexion transparente des deux réseaux en sorte que toute machine de l'un des réseaux peut communiquer avec une machine de l'autre réseau.

Authentification : Le routeur qui établit le VPN est authentifié par celui qui l'accepte et toute autre connexion est rejetée.

Confidentialité : Les données sont cryptées.

On choisira IPSec lorsque le routeur IPL-C doit établir un VPN avec un serveur VPN IPSec déjà installé.

On préfèrera OpenVPN lorsque le trafic VPN doit être routé au travers de routeurs intermédiaires pour profiter de la grande souplesse de cette technique.

Serveur RAS pour PC, tablette et smartphone
Le routeur IPL-C fait également fonction de serveur d'accès distant permettant à un groupe d'utilisateurs distants enregistrés dans la liste d'utilisateurs d'accéder aux machines du réseau avec des droits maîtrisés.

De plus, le portail HTTPS accueille les utilisateurs de PC, tablettes et smartphones en mode HTTPS pour les rediriger en sécurité vers les serveurs HTTPS ou HTML que leur identité autorise.

Firewall
Le routeur IPL-C dispose d'un firewall « SPI » qui inspecte les paquets en permanence.

Il permet de rejeter les tentatives de connexions non authentifiées sur l'Internet.

Il permet également d'attribuer des droits maîtrisés (@IP et N° de port de destination autorisés) aux trames IP reçues au travers d'un tunnel VPN.

Redondance VRRP en cas de panne du routeur :
En cas de panne, le routeur IPL-C peut se déclarer en stand-by en sorte qu'un autre routeur prenne le relais avec un fonctionnement identique.

Interface WiFi optionnel (point d'accès ou client)
Le routeur IPL-C peut être équipé d'une interface WiFi 2.4 et 5GHz.
L'interface WiFi peut fonctionner comme point d'accès pour permettre le raccordement de clients WiFi (automate équipé d'une interface WiFi, tablette, Webcam …) ou bien en client WiFi.

SNMP
Le routeur IPL-C est agent SNMP; il répond à la MIB2 standard et transmet un trap SNMP lorsque des événements paramétrables surviennent.

PRESENTATION

DNS
Le système DNS permet au routeur IPL-C d'établir une connexion avec un autre routeur même si l'un, l'autre ou les deux routeurs ne possèdent pas une adresse IP connue.
Le principe du DNS consiste à désigner un routeur destinataire d'une connexion par un nom de domaine (par exemple « etictelecom » est un nom de domaine) plutôt que par son adresse IP.

Serveur DHCP
Sur l'interface LAN, le routeur IPL-C peut se comporter en serveur DHCP.

Emails – sms
Un email enregistré dans le routeur peut être transmis lorsque l'entrée tout ou rien se ferme ou s'ouvre.
Cet email peut être transformé en SMS si l'adresse mail du destinataire a été attribuée à un numéro de téléphone mobile.

Configuration HTML, TTPS, SSH
Le routeur IPL-C se configure au moyen d'un navigateur HTML (ou HTTPS).

EticFinder
Le logiciel ETICFinder livré avec le routeur ; il permet de détecter simplement tous les produits de marque ETIC connectés à un segment Ethernet pour afficher leur adresse MAC ainsi que l'adresse IP qui leur est attribuée sur le réseau.

Passerelle série
Certaines références du routeur possèdent une passerelle série (RS232 ou RS485 ou RS422 ou USB).
La passerelle fonctionne suivant l'un des modes suivants :

Raw TCP client ou serveur
Raw UDP
Telnet
Modbus maître ou esclave
Unitelway

3.3 Organisation du routeur

Interface WAN du routeur
L'interface WAN est normalement l'interface cellulaire.

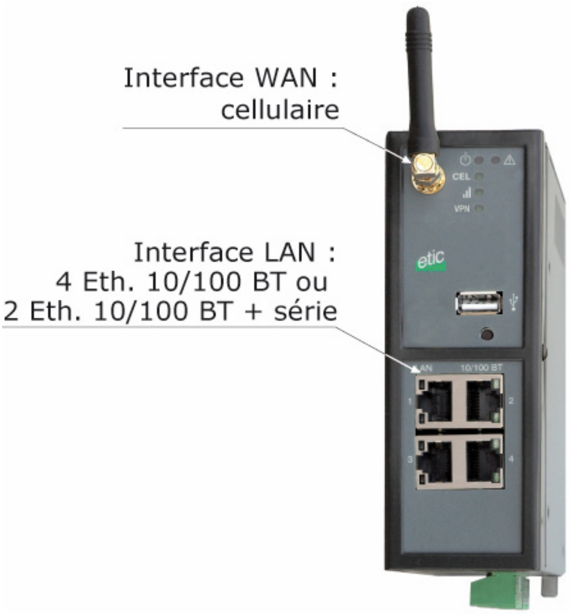
Cependant, pour permettre une utilisation plus étendue du routeur, l'interface cellulaire peut être remplacée par l'interface Ethernet 10/100 BT de la prise RJ45 N°1 du routeur, pour y raccorder un modem, par exemple, ou bien par l'interface WiFi.
Une seule interface WAN peut être utilisée à la fois.

Interface LAN du routeur
L'interface LAN est constituée de 2 ou 4 prises Ethernet switchées.
Les équipements de l'interface LAN constituent le réseau LAN.
L'interface LAN peut comporter en option 1 ou 2 interfaces série RS232, RS485 ou RS422 et le WiFi.

Réseau LAN
Les équipements de l'interface LAN constituent le réseau LAN.

Firewall
Les opérations de filtrage du firewall sont réalisées entre l'interface WAN et l'interface LAN

Serveur d'accès distant
Les utilisateurs distants sont accueillis sur l'interface WAN.



4 Fiche technique

Caractéristiques générales	
Dimensions	137 x 48 x 116 mm (h, l, p)
EMI	EN50082-2
Sécurité électrique	EN 60950- UL 1950
CEM	ESD : EN61000-4-2 : Décharge 6 KV Champ HF : EN61000-4-3 : 10V/m < 2 GHz Transitoires : EN61000-4-4 Choc : EN61000-4-5 : 4KV line / earth
Substances dangereuses	2002/95/CE (RoHS)
Tension d'alimentation	IPL-C-400, IPL-CW-400 10 à 60 VDC IPL-C-230, IPL-CW-230 10 à 60 VDC IPL-C-260, IPL-CW-260 10 à 60 VDC IPL-C-261, IPL-CW-261 10 à 60 VDC IPL-C-220, IPL-CW-220 10 à 30 VDC
Puissance absorbée	6W
T° d'utilisation	-20°C / + 60°C Humidité 5 à 95 %

Réseau cellulaire	
Type	4G / 3G+ / GPRS-EDGE selon modèle
Connecteur Antenne	SMA femel

Type de la carte cellulaire CODE 3	LE	LS	LA	HG
4G	**Europe**	**USA**	**Asie**	-
3G+	**Oui (*1)**	**Oui (*1)**	**Oui (*1)**	**Oui (*2)**
GPRS-EDGE	**Oui (*3)**	**Oui (*3)**	**Oui (*3)**	**Oui (*3)**

(*1) 850 / 900 / 1900 / 2100 MHz
(*2) 850 / 900 / 1700 / 1900 / 2100 MHz
(*3) 850 / 900 / 1800 / 1900 MHz

Réseau WiFI	
Type	2.4 et 5 GHz
Connecteur Antenne	R-SMA femelle
Normes de transmission	802.11 a/b/g/n

Liaison série	
RS232-RS485	1200 à 115200 kb/s parity N / E / O
Passerelle RS232	Raw client et serveur - Modbus maître et esclave Multicast - Telnet - Unitelway
USB	1 port USB host Client PPP sur l'interface USB

Ethernet / routage IP	
Ethernet	10-100 BT Détection de débit 10 ou 100 Mb/s et de câble croisé
Routeur	Connexions distantes - Routes statiques - RIP V2
Translation d'@IP	Translation d'@IP source (NAT) Translation d'@IP destination (DNAT) Translation de port (Port forwarding) Substitution d'@ IP source et destination (version B seulement)
DNS	Gestion du système de nom de domaine
DHCP	Internet : Client ou @IP fixe LAN : DHCP client ou serveur ou @ IP fixe

Sécurité	
VPN	Client ou serveur IPSEC ou TLS/SSL 25 VPN simultanés cryptage AES256 ou 3DES Authentification IPSec : Clé partagée ou certificat X509 Authentification TLS : Certificat X509
Firewall	Stateful packet inspection (50 règles) Filtrage d'adresses IP et des N° de port source et destination
Logs	Tableau d'événements horodatés

Serveur d'accès distant (RAS)	
Utilisateurs distants	Liste de 25 utilisateurs
Connexion	Sécurisée par VPN PPTP / L2TP-IPSec / TLS Open VPN Contrôle de Login et mot de passe Contrôle de certificat X509
M2Me	Compatible du logiciel client VPN M2Me_Secure Compatible du service de médiation M2Me_Connect
Alarmes	Email au moyen d'1 entrée numérique

Liaison série	
RS232-RS485	1200 à 115200 kb/s parity N / E / O
Passerelle RS232	Raw client et serveur - Modbus maître et esclave Multicast - Telnet - Unitelway
USB	1 port USB host Client PPP sur l'interface USB

Redondance et secours de liaison	
Redondance en cas de panne du routeur	VRRP et OSPF permettent de placer deux routeurs en backup l'un de l'autre
Liaison de secours	Par modem 3G externe

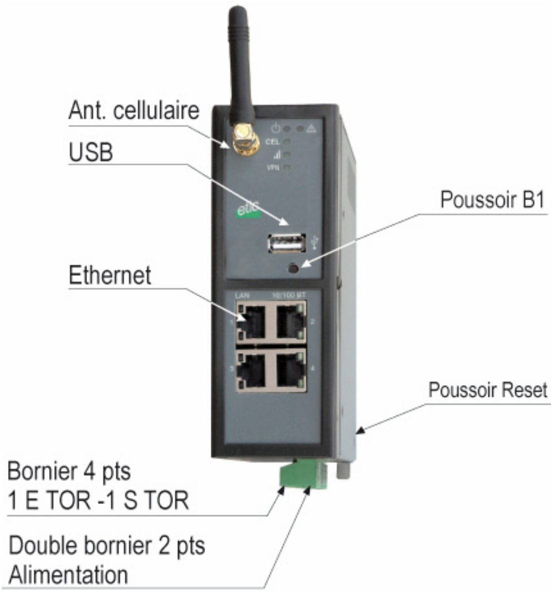
1 Description du produit

1.1 Dimensions

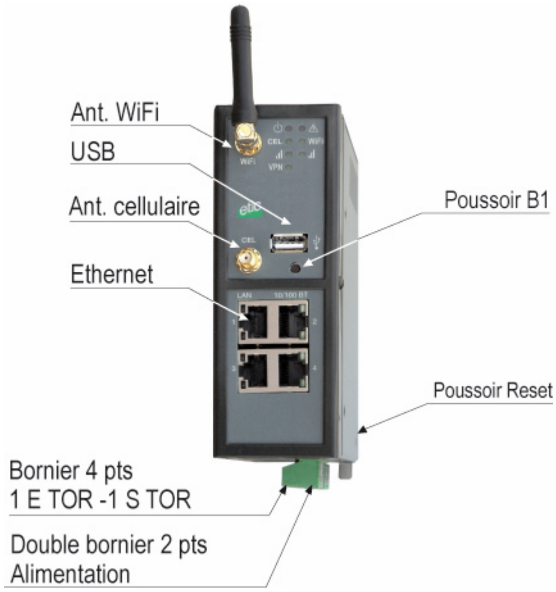


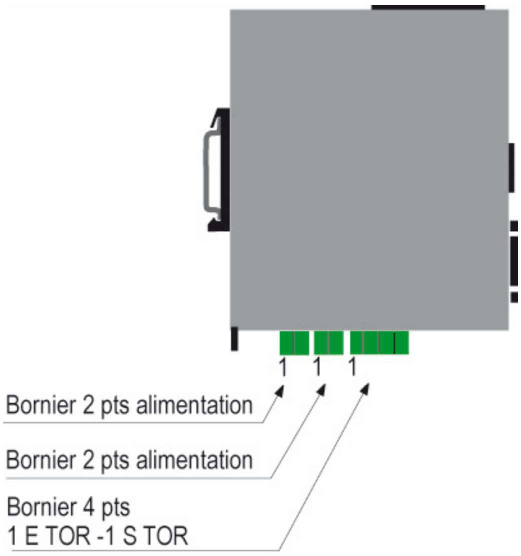
1.2 Routeur IPL-C-400 ou IPL-CW-400 (option WiFi)

IPL-C-400



IPL-CW-400





VOYANTS IPL-C-400 et IPL-CW-400			
	Désignation	**Fonction**	
Opération		Vert : Rouge : Rouge clignotant lent Rouge clignotant rapide	En fonction Carte SIM non présente ou non détectée ou code PIN erroné Erreur de démarrage grave ou erreur chargement firmware Alarme matérielle Chargement du firmware en cours
Connexion Cellulaire	**Cel**	Eteint Impulsion toutes les 4 s Clignotant lent 2 s Clignotant rapide 0,5 s Vert	Carte SIM absente - code PIN erroné – interf. cell. inactif Interface cellulaire actif non connectée (état temporaire) Connexion en cours 1ere étape Connexion en cours 2eme étape (mot de passe et @ IP) Connecté / léger clignotement en présence de data
Qualité du signal cellulaire	**Cel**	Eteint : 1 impulsion 2 impulsions 3 impulsions Voir détail au paragraphe installation de l'antenne	Pas de signal mesuré Insuffisant ou faible Suffisant Bon ou très bon signal
	VPN	Un VPN au moins est établi	
Connexion WiFi	**WiFi**	Eteint Clignotant lent Clignotant rapide Vert	Ligne non connectée ou WiFi configuré en point d'accès Connexion en cours 1ere étape / détection en cours Connexion en cours 2 eme étape / Echange identifiants et IP Connecté avec léger clignotement en présence de data
Qualité du signal WiFi	**WiFi**	Eteint 1 impulsion 2 impulsions 3 impulsions	Pas de signal mesuré ou WiFi configuré en point d'accès Insuffisant ou faible Suffisant Bon ou très bon signal
Voyant inférieur	**Ethernet 1 à 4**	Eteint Vert	Interface désactivé Interface actif / léger clignotement en présence de data
Voyant supérieur	**Ethernet 1**	Vert	La RJ45 N°1 a été configuré comme interface WAN

Bouton poussoir de face avant B1 Autoriser temporairement l'accès distant		
Appui Sur BP1	**Voyant**	**Fonction**
5 secondes	3 impulsions en vert	La hotline d'ETIC TELECOM est autorisée à établir une connexion distante OpenVPN vers le routeur IPL. La connexion distante doit intervenir dans un délai de 1 heure.
10 secondes	5 impulsions en vert	Un utilisateur distant est autorisé à établir une connexion distante OpenVPN vers le routeur IPL sans identificateur / mot de passe d'utilisateur distant. La connexion distante doit intervenir dans un délai de 10 mn. L'accès est limité au serveur de configuration du routeur IPL

Bouton poussoir de face arrière Pour lever temporairement la sécurité d'accès au serveur de configuration du routeur		
Appui sur BP de face arrière	**Voyant**	**Fonction**
pendant le fonctionnement	Clignotement rouge	Retour à l'adresse IP usine 192.168.0.128 La configuration courante reste active.
Simultanément avec la mise sous tension	Clignotement rouge	Retour à la configuration Usine La configuration courante est perdue sauf si elle a été sauvegardée dans un fichier.

Bornier 2 points : Alimentation 1 (C1) Point 1 à l'arrière – Alimentation protégée contre l'inversion de polarité		
Broche	**Signal**	**Fonction**
1	Power 1 +	Alimentation 1
2	Power 1 -	0V isolé du châssis

Bornier 2 points : Alimentation 2 (C2) Point 1 à l'arrière – Alimentation protégée contre l'inversion de polarité		
Broche	**Signal**	**Fonction**
1	Power 1 +	Alimentation 2
2	Power 1 -	0V isolé du châssis

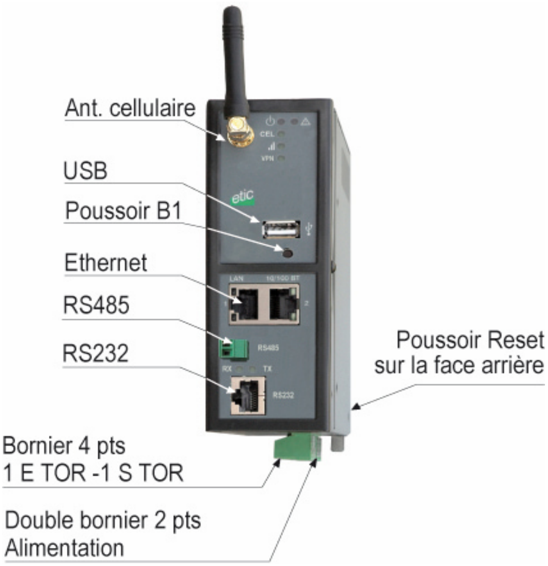
Bornier 4 points : Entrée-Sortie TOR (C3) Point 1 à l'arrière		
Broche	**Signal**	**Fonction**
1	0V	Tension + 3 V DC fournie par le produit
2	In	Entrée TOR
3	F +	Sortie TOR + (max 50Vdc - 0,6A)
4	F -	Sortie TOR -

Connecteur RJ45 Ethernet 1 à 4 (C6 à C9)		
Broche	**Signal**	**Fonction**
1	Tx +	Emission polarité +
2	Tx -	Emission polarité -
3	Rx +	Réception polarité +
4	N.C	-
5	N.C	-
6	Rx -	Réception polarité -
7	N.C.	-
8	N.C.	-

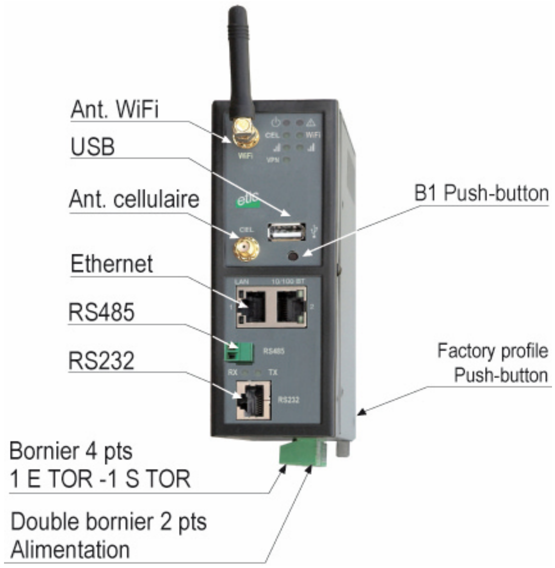
Connecteurs d'antennes Attention : les connecteurs pour réseau cellulaire et WiFi sont différents		
Réseau	**Type**	**Observation**
Cellulaire	SMA femelle	2 antennes peuvent être connectées pour améliorer la transmission 4G (modèle LE)
WiFi	RP-SMA femelle	1 connecteur à polarité inversée conforme à l'usage pour le raccordement des antennes WiFi

1.3 Routeur IPL-C-220 ou IPL-CW-220 (option WiFi)

IPL-C-220



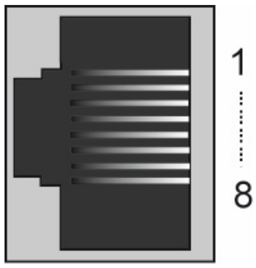
IPL-CW-220

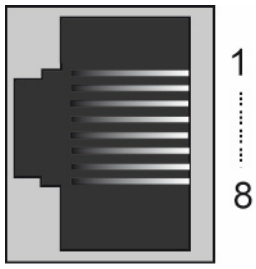


VOYANTS IPL-C-220 et IPL-CW-220			
	Désignation	**Fonction**	
Opération	⏻	Vert : Rouge : Rouge clignotant lent Rouge clignotant rapide	En fonction Carte SIM non présente ou non détectée ou code PIN erroné Erreur de démarrage grave ou erreur chargement firmware Alarme matérielle Chargement du firmware en cours
Connexion Cellulaire	**Cel**	Eteint Impulsion toutes les 4 s Clignotant lent 2 s Clignotant rapide 0,5 s Vert	Carte SIM absente - code PIN erroné - interface cellulaire inactif Interface cellulaire actif non connectée (état temporaire) Connexion en cours 1ere étape Connexion en cours 2eme étape (mot de passe et @ IP) Connecté / léger clignotement en présence de data
Qualité du signal cellulaire	**Cel**	Eteint : 1 impulsion : 2 impulsions : 3 impulsions : Voir détail dans tableau ci-dessous	Pas de signal mesuré Insuffisant ou faible Suffisant Bon ou très bon signal
	VPN	Un VPN au moins est établi	
Connexion WiFi	**WiFi**	Eteint : Clignotant lent : Clignotant rapide : Vert	Ligne non connectée ou WiFi configuré en point d'accès Connexion en cours 1ere étape / détection en cours Connexion en cours 2 eme étape / Echange identifiants et IP Connecté / léger clignotement en présence de data
Qualité du signal WiFi	**WiFi**	Eteint : 1 impulsion : 2 impulsions : 3 impulsions :	Pas de signal mesuré ou WiFi configuré en point d'accès Insuffisant ou faible Suffisant Bon ou très bon signal
Voyant inférieur	**Ethernet 1 à 4**	Eteint : Vert :	Interface désactivé Connecté / léger clignotement en présence de data
Voyant supérieur	**Ethernet 1**	Eclairé :	La RJ45 N°1 a été configurée comme interface WAN
RS232 **RS485**	**Rx**	Caractères reçus de la liaison V24/RS232 (vers IPL)	
	Tx	Caractères transmis vers la liaison V24/RS232 (depuis IPL)	

Connecteurs et borniers Alimentation (C1 & C2), Entrée-Sortie TOR (C3) et Ethernet (C6 à C9)
Ces éléments sont communs à tous les modèles **On trouvera le brochage de ces connecteurs au paragraphe 4.1**

Bornier 2 points RS485 (C10)		
Broche	**Signal**	**Fonction**
1	A	RS485 polarité A
2	B	RS485 polarité B

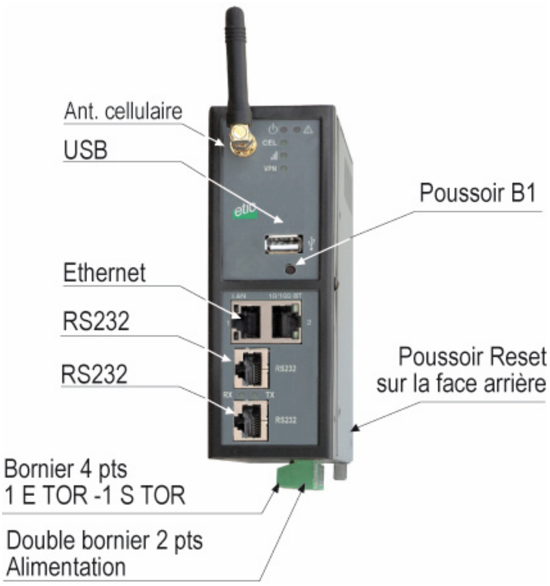
Connecteur RJ45 RS232 (C11, C12) Raccordement d'un équipement DCE				
Broche	**Signal**	**Sens**	**Fonction**	**Brochage de l'embase RJ45**
1	DTR - 108	Sortie	Terminal de données prêt	
2	TD - 103	Sortie	Emission de données	
3	RD - 104	Entrée	Réception de données	
4	DSR - 107	Entrée	Poste de données prêt	
5	SG - 102	-	Terre de signalisation	
6	Inutilisé	Sortie	-	
7	CTS - 106	Entrée	Prêt à émettre	
8	RTS - 105	Sortie	Demande pour émettre	

Connecteur RJ45 RS232 (C11, C12) Raccordement d'un équipement DCE				
Broche	**Signal**	**Sens**	**Fonction**	**Brochage de l'embase RJ45**
1	CD - 109	Sortie	Détection de porteuse	
2	RD - 104	Sortie	Réception de données	
3	TD - 103	Entrée	Emission de données	
4	DTR - 108	Entrée	Terminal de données prêt	
5	SG - 102	-	Terre de signalisation	
6	DSR - 107	Sortie	Poste de données prêt	
7	RTS - 105	Entrée	Demande pour émettre	
8	CTS - 106	Sortie	Prêt à émettre	

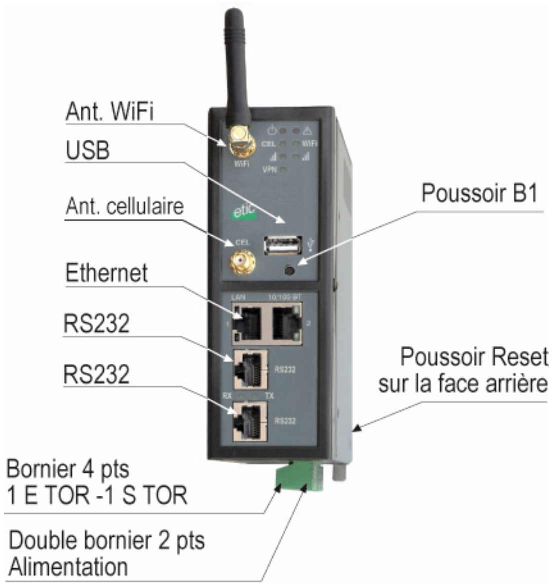
Sortie = Signal fourni par le routeur.
Entrée = Signal fourni par l'équipement extérieur.

1.4 Routeur IPL-C-230 ou IPL-CW-230 (option WiFi)

IPL-C-230

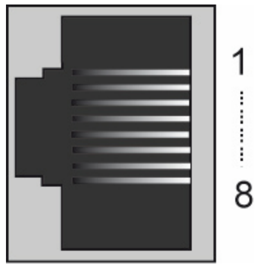


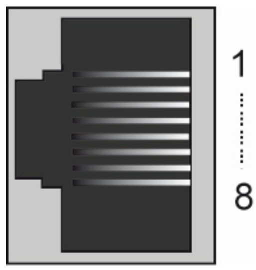
IPL-CW-230



VOYANTS IPL-C-230 et IPL-CW-230			
	Désignation	**Fonction**	
Opération	⏻	Vert Rouge Clignotant rouge lent Clignotant rouge rapide	En fonction Carte SIM non présente ou non détectée ou code PIN erroné Erreur de démarrage grave ou erreur chargement firmware Alarme matérielle Chargement du firmware en cours
Connexion Cellulaire	**Cel**	Eteint Impulsion toutes les 4 s Clignotant lent 2 s Clignotant rapide 0,5 s Vert	Carte SIM absente - code PIN erroné - interface cellulaire inactif Interface cellulaire actif non connectée (état temporaire) Connexion en cours 1ere étape Connexion en cours 2eme étape (mot de passe et @ IP) Connecté avec léger clignotement en présence de data
Qualité du signal cellulaire	**Cel**	Eteint 1 impulsion 2 impulsions 3 impulsions	Pas de signal mesuré Insuffisant ou faible Suffisant Bon ou très bon signal
	VPN	Un VPN au moins est établi	
Connexion WiFi	**WiFi**	Eteint Clignotant lent Clignotant rapide Vert	Ligne non connectée ou WiFi configuré en point d'accès Connexion en cours 1ere étape / détection en cours Connexion en cours 2 eme étape / Echange identifiants et IP Connecté avec léger clignotement en présence de data
Qualité du signal WiFi	**WiFi**	Eteint : 1 impulsion 2 impulsions 3 impulsions	Pas de signal mesuré ou WiFi configuré en point d'accès Insuffisant ou faible Suffisant Bon ou très bon signal
Voyant inférieur	**Ethernet 1 à 4**	Eteint Vert	Interface désactivé Connecté avec léger clignotement en présence de data
Voyant supérieur	**Ethernet 1**	Eclairé	La RJ45 N°1 a été configurée comme interface WAN
RS232	**Rx**	Caractères reçus de la liaison V24/RS232 (vers IPL)	
	Tx	Caractères transmis vers la liaison V24/RS232 (depuis IPL)	

Connecteurs et borniers Alimentation (C1 & C2), Entrée-Sortie TOR (C3), et Ethernet (C6 à C9)
Ces éléments sont communs à tous les modèles **On trouvera le brochage de ces connecteurs au paragraphe relatif au modèle de base IPL-C-400**

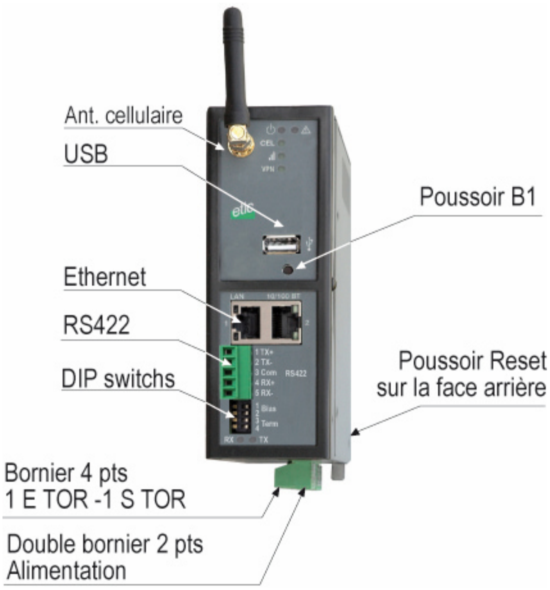
Connecteur RJ45 RS232 (C11, C12) Raccordement d'un équipement DCE				
Broche	**Signal**	**Sens**	**Fonction**	**Brochage de l'embase RJ45**
1	DTR - 108	Sortie	Terminal de données prêt	
2	TD - 103	Sortie	Emission de données	
3	RD - 104	Entrée	Réception de données	
4	DSR - 107	Entrée	Poste de données prêt	
5	SG - 102	-	Terre de signalisation	
6	Inutilisé	Sortie	-	
7	CTS - 106	Entrée	Prêt à émettre	
8	RTS - 105	Sortie	Demande pour émettre	

Connecteur RJ45 RS232 (C11, C12) Raccordement d'un équipement DCE				
Broche	**Signal**	**Sens**	**Fonction**	**Brochage de l'embase RJ45**
1	CD - 109	Sortie	Détection de porteuse	
2	RD - 104	Sortie	Réception de données	
3	TD - 103	Entrée	Emission de données	
4	DTR - 108	Entrée	Terminal de données prêt	
5	SG - 102	-	Terre de signalisation	
6	DSR - 107	Sortie	Poste de données prêt	
7	RTS - 105	Entrée	Demande pour émettre	
8	CTS - 106	Sortie	Prêt à émettre	

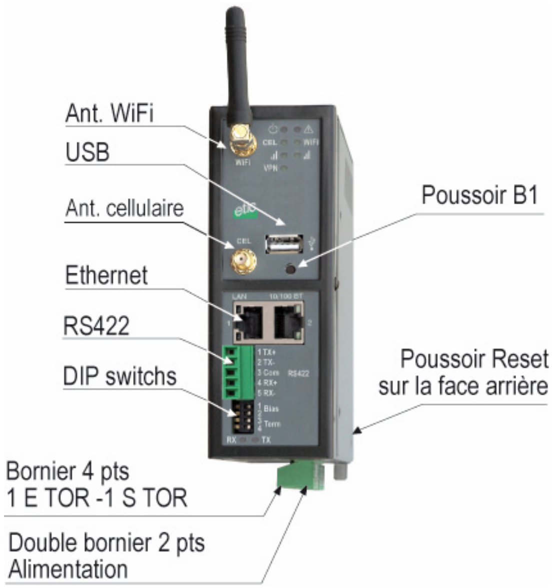
Sortie = Signal fourni par le routeur.
Entrée = Signal fourni par l'équipement extérieur.

1.5 Routeur IPL-C-260 ou IPL-CW-260 (option WiFi)

IPL-C-260



IPL-CW-260



VOYANTS IPL-C-260 et IPL-CW-260			
	Désignation	**Fonction**	
Opération	⏻	Vert : Rouge : Rouge clignotant lent Rouge clignotant rapide	En fonction Carte SIM non présente ou non détectée ou code PIN erroné Erreur de démarrage grave ou erreur chargement firmware Alarme matérielle Chargement du firmware en cours
Connexion Cellulaire	**Cel**	Eteint Impulsion toutes les 4 s Clignotant lent 2 s Clignotant rapide 0,5 s Vert	Carte SIM absente - code PIN erroné – interf. cell. inactif Interface cellulaire actif non connectée (état temporaire) Connexion en cours 1ere étape Connexion en cours 2eme étape (mot de passe et @ IP) Connecté / léger clignotement en présence de data
Qualité du signal cellulaire	**Cel**	Eteint : 1 impulsion : 2 impulsions : 3 impulsions : Voir détail dans tableau ci-dessous	Pas de signal mesuré Insuffisant ou faible Suffisant Bon ou très bon signal
	VPN	Un VPN au moins est établi	
Connexion WiFi	**WiFi**	Eteint Clignotant lent Clignotant rapide Vert	Ligne non connectée ou <u>WiFi configuré en point d'accès</u> Connexion en cours 1ere étape / détection en cours Connexion en cours 2 eme étape / Echange identifiants et IP Connecté avec léger clignotement en présence de data
Qualité du signal WiFi	**WiFi**	Eteint 1 impulsion 2 impulsions 3 impulsions	Pas de signal mesuré ou <u>WiFi configuré en point d'accès</u> Insuffisant ou faible Suffisant Bon ou très bon signal
Voyant inférieur	**Ethernet 1 à 4**	Eteint Vert	Interface désactivé Interface actif / léger clignotement en présence de data
Voyant supérieur	**Ethernet 1**	Eclairé :	La RJ45 N°1 a été configurée comme interface WAN
RS422	**Rx**	Caractères reçus de la liaison V24/RS232 (vers IPL)	
	Tx	Caractères transmis vers la liaison V24/RS232 (depuis IPL)	

Connecteurs et borniers Alimentation (C1 & C2), Entrée-Sortie TOR (C3), Ethernet (C6 à C9)
Ces éléments sont communs à tous les modèles **On trouvera le brochage de ces connecteurs au paragraphe relatif au modèle de base IPL-C-400**

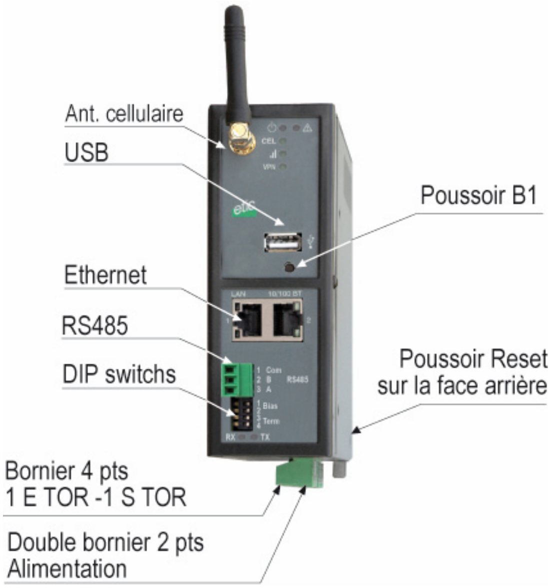
Bornier 5 points : RS422 (C13)			
Broche	**Signal**		**Fonction**
1	TX+	Sortie	Emission RS422 polarité +
2	TX-	Sortie	Emission RS422 polarité -
3	Com		Commun
4	RX+	Entrée	Réception RS422 polarité +
5	RX-		Réception RS422 polarité -

Sortie = Signal fourni par le routeur.
Entrée = Signal fourni par l'équipement extérieur.

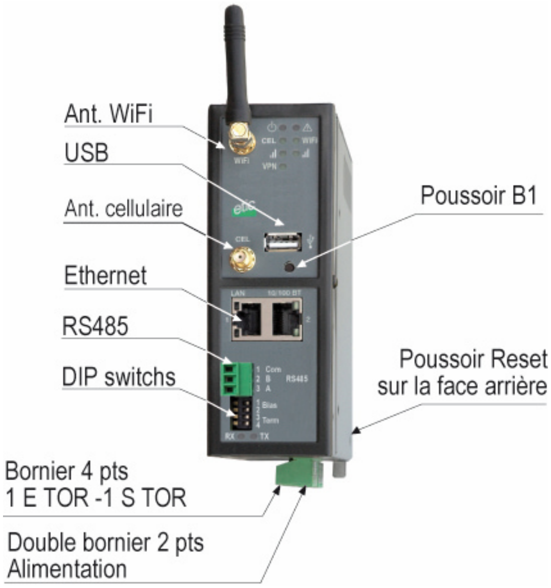
Micro-switches RS422		
SW 1	**SW 2**	
ON	ON	Signal de réception RS422 polarisé par des résistances de 470 Ohms
OFF	OFF	Signal de réception RS422 non polarisé
SW3	**SW4**	
ON	ON	Résistance 120 Ohm de terminaison de ligne réception en service
OFF	OFF	Résistance 120 Ohm de terminaison de ligne réception hors service

1.6 Routeur IPL-C-261 ou IPL-CW-261 (option WiFi)

IPL-C-261



IPL-CW-261



VOYANTS IPL-C-261 et IPL-CW-261			
	Désignation	**Fonction**	
Opération	⏻	Vert : Rouge : Rouge clignotant lent Rouge clignotant rapide	En fonction Carte SIM non présente ou non détectée ou code PIN erroné Erreur de démarrage grave ou erreur chargement firmware Alarme matérielle Chargement du firmware en cours
Connexion Cellulaire	**Cel**	Eteint Impulsion toutes les 4 s Clignotant lent 2 s Clignotant rapide 0,5 s Vert	Carte SIM absente - code PIN erroné – interf. cell. inactif Interface cellulaire actif non connectée (état temporaire) Connexion en cours 1ere étape Connexion en cours 2eme étape (mot de passe et @ IP) Connecté / léger clignotement en présence de data
Qualité du signal cellulaire	**Cel**	Eteint : 1 impulsion 2 impulsions 3 impulsions	Pas de signal mesuré Insuffisant ou faible Suffisant Bon ou très bon signal
	VPN	Un VPN au moins est établi	
		Eteint Clignotant lent Clignotant rapide Vert	Ligne non connectée ou <u>WiFi configuré en point d'accès</u> Connexion en cours 1ere étape / détection en cours Connexion en cours 2 eme étape / Echange identifiants et IP Connecté avec léger clignotement en présence de data
Connexion WiFi	**WiFi**	Eteint 1 impulsion 2 impulsions 3 impulsions	Pas de signal mesuré ou <u>WiFi configuré en point d'accès</u> Insuffisant ou faible Suffisant Bon ou très bon signal
Qualité du signal WiFi	**WiFi**	Eteint Vert	Interface désactivé Interface actif / léger clignotement en présence de data
Voyant inférieur	**Ethernet 1 à 4**	Vert : Rouge : Rouge clignotant lent Rouge clignotant rapide	En fonction Carte SIM non présente ou non détectée ou code PIN erroné Erreur de démarrage grave ou erreur chargement firmware Alarme matérielle Chargement du firmware en cours
Voyant supérieur	**Ethernet 1**	Eclairé :	La RJ45 N°1 a été configurée comme interface WAN
RS485	**Rx**	Caractères reçus de la liaison V24/RS232 (vers IPL)	
	Tx	Caractères transmis vers la liaison V24/RS232 (depuis IPL)	

Connecteurs et borniers Alimentation (C1 & C2), Entrée-Sortie TOR (C3), Ethernet (C6 à C9)
Ces éléments sont communs à tous les modèles
On trouvera le brochage de ces connecteurs au paragraphe relatif au modèle de base IPL-C-400

Bornier RS485 isolé (C14)		
Broche	**Signal**	**Fonction**
1	Com	Commun isolé
2	B (+)	RS485 polarité B
3	A (-)	RS485 polarité A

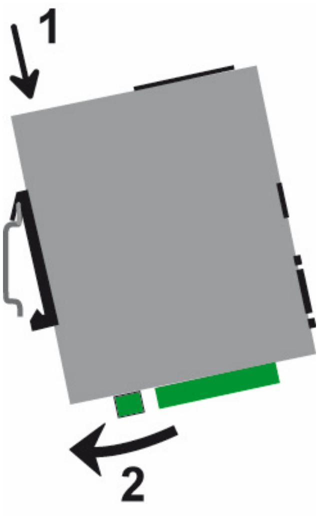
Micro-switches RS485		
SW 1	**SW 2**	
ON	ON	Signal polarisé par des résistances de 470 Ohms
OFF	OFF	Signal non polarisé
SW3	**SW4**	
ON	ON	Résistance 120 Ohm de terminaison de ligne en service
OFF	OFF	Résistance 120 Ohm de terminaison de ligne hors service

2 Installer le routeur sur un rail DIN 35 mm

Pour installer le produit sur un rail Din 35 mm,

- Incliner le produit.
- Engager le produit dans la partie supérieure du rail.
- Pousser pour encliqueter.

Laisser un espace d'environ 1 cm de part et d'autre du routeur pour faciliter l'écoulement de la chaleur.



Pour démonter le produit du rail Din 35 mm,

- Pousser légèrement vers le bas.
- Dégager le produit vers l'avant



3 Alimentation

Le produit est pourvu de 2 entrées d'alimentation . permettant la connexion de deux sources d'alimentation pouvant agir en secours l'une de l'autre.
En cas de défaillance d'une source, l'autre prend le relais.

IPL-C-400, IPL-CW-400 **IPL-C-230, IPL-CW-230** **IPL-C-260, IPL-CW-260** **IPL-C-261, IPL-CW-261**	Tension minimum : 9 V continu Tension maximum = 60 V continu
IPL-C-220, IPL-CW-220	Tension minimum : 9 V continu Tension maximum = 30 V continu

La consommation est de 7W.

4 Ventilation

Le produit est conçu pour être fixé sur un rail DIN 35 mm.

Pour éviter tout échauffement, en particulier lorsque la température ambiante peut s'élever dans l'armoire électrique, on veillera à ménager un espace de 1 cm de chaque côté du produit pour faciliter l'écoulement de la chaleur.

5 Mise à la terre

Le boîtier est métallique; on veillera à relier la cosse de mise à la terre du boîtier (située sur sa face inférieure) à une terre de protection efficace.

6 Connexions RJ45 Ethernet 10/100

Les interfaces Ethernet sont à reconnaissance automatique du débit 10 ou 100 Mb/s et de croisement de circuits.

Pour connecter directement un PC au routeur (par exemple, à la mise en service), utiliser un cordon Ethernet standard croisé ou non.

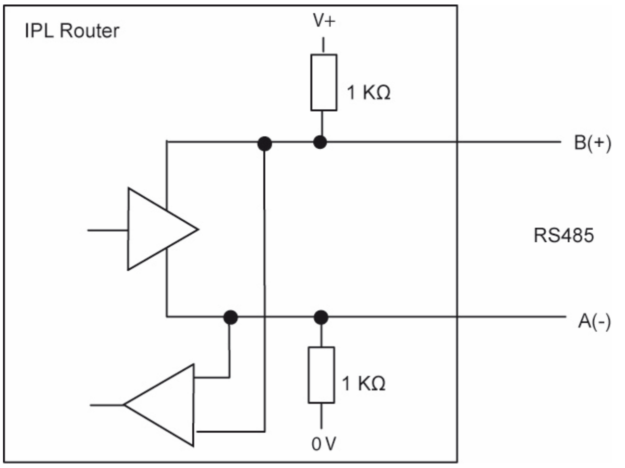
7 Connexion à l'interface RS232 (IPL-C-220 ou IPL-C-230)

Le routeur IPL-C-230 dispose de deux interfaces série RS232.
Les produits IPL-C-220 dispose d'une interface série RS232 et d'une interface RS485.
Ces interfaces permettent le raccordement d'un équipement asynchrone (automate …) afin de pouvoir y accéder depuis le réseau local ou à distance
.
Liaison RS232
La liaison RS232 permet de raccorder indifféremment un équipement DTE (terminal) ou DCE (modem). Selon le type d'équipement à raccorder, utiliser l'un des câbles suivants (à commander séparément) :

Câbles RS232		
Référence	**Connecteur**	**Fonction**
CAB592	SubD 9 pts male	Raccordement d'un DCE
CAB593	SubD 9 pts femelle	Raccordement d'un DTE
CAB609	Fils nus	Raccordement d'un DTE ou DCE selon câblage

Longueur maximale du câble RS232
L'équipement raccordé à l'interface RS232 ne doit pas être éloigné de plus d'une dizaine de mètres et le câble de raccordement doit de préférence être blindé.

8 Connexion à l'interface RS485 (IPL-C-220)



L'interface RS485 du routeur IPL-C-220 n'est pas isolée. Elle est polarisée par des résistances de 1 KOhm à l'intérieur du produit.

Si les équipements RS485 sont à raccordés à une distance supérieure à 10m, on aura soin de connecter une résistance de terminaison de ligne et deux résistances de polarisation suivant les règles de l'art.

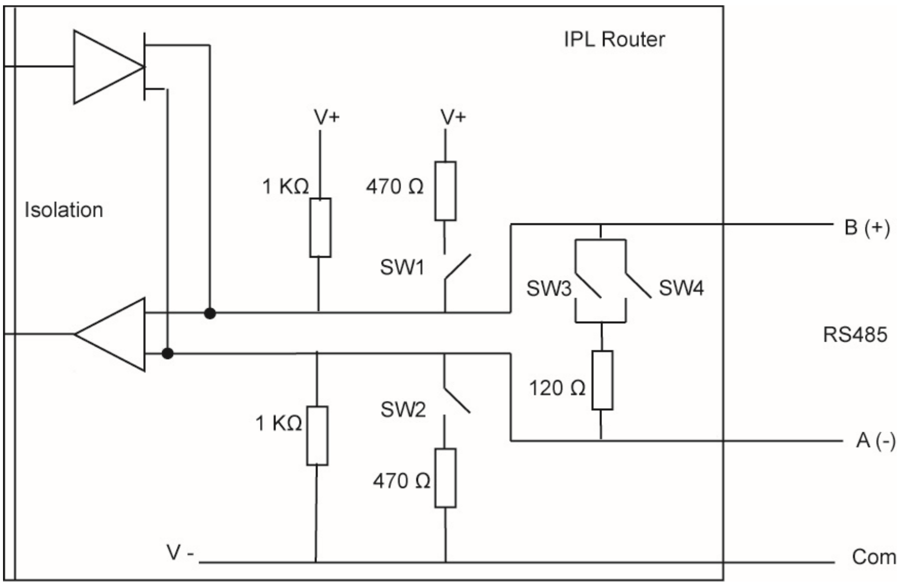
9 Connexion série RS422 isolé (IPLC-260)

L'interface RS422 du routeur IPL-C-260 est isolée (4 fils).

Les résistances de terminaison et de polarisation peuvent être sélectionnées par des DIP switches.
La résistance de terminaison de 120 Ohm doit être activée si le routeur est placé à l'extrémité du bus RS422.
Les résistances de polarisation doivent être activées par l'un des équipements du bus.
16 équipements RS422 peuvent être raccordés au routeur.
Si possible, on utilisera du câble torsadé par paire et blindé.

L'interface RS422 permet de transmettre sur la distance maximum possible pour ce type d'interface soit environ 1000 mètres environ au débit de 9600 b/s avec une paire torsadée et un fil de diamètre 0,8 mm.

Dans le cas ou plus d'un équipement est raccordé au routeur, le routeur IPL-C doit être maître sur le bus RS422; ainsi, Il ne peut pas y avoir d'autres émetteurs RS422 raccordés sur la paire d'émission (TX+ et TX-) de l'interface.



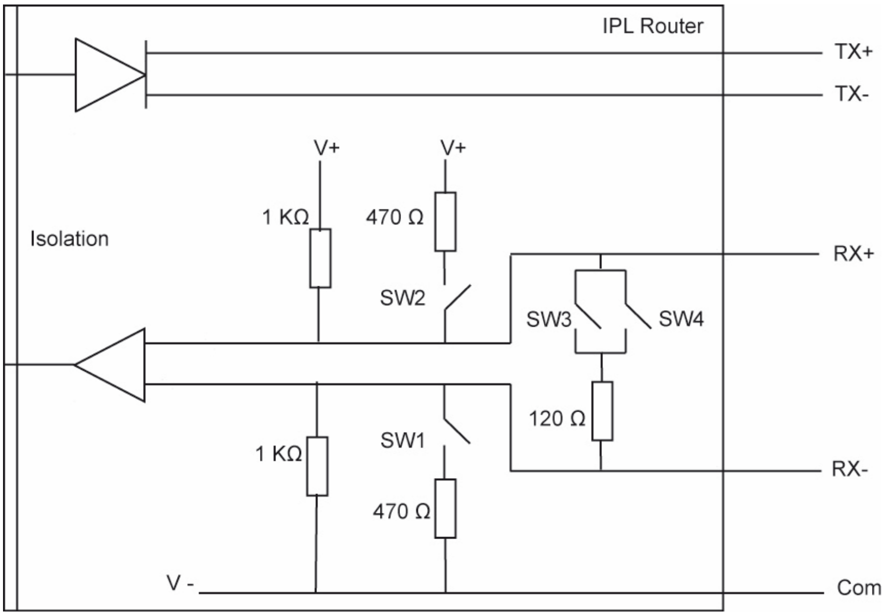
Si la ligne est exposée à l'orage, l'utilisation de para-surtenseurs est recommandée.

10 Connexion série RS485 isolée (IPL-C-261)

L'interface série RS485 du routeur IPL-C-261 est isolée (2 fils + 1 commun).

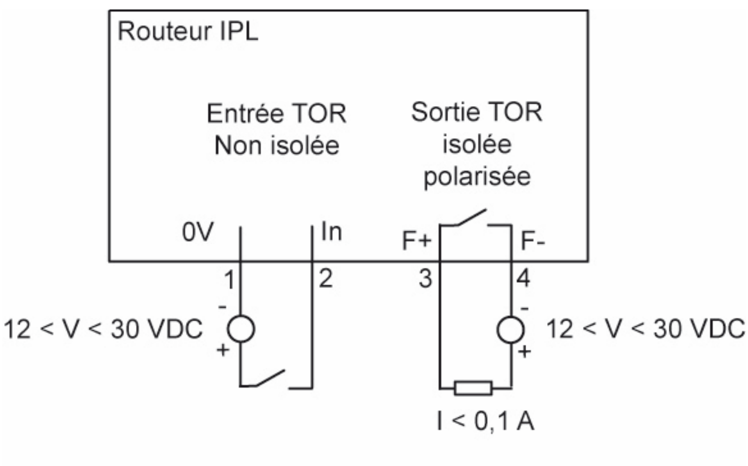
Les résistances de terminaison et de polarisation peuvent être sélectionnées par des DIP switches.
La résistance de terminaison de 120 Ohm doit être activée si le routeur est placé à l'extrémité du bus RS485.
Les résistances de polarisation doivent être activées par l'un des équipements du bus.
16 équipements RS485 peuvent être raccordés au routeur.
Si possible, on utilisera du câble torsadé par paire et blindé.

L'interface RS422 permet de transmettre sur la distance maximum possible pour ce type d'interface soit environ 1000 mètres environ au débit de 9600 b/s avec une paire torsadée et un fil de diamètre 0,8 mm.



Si la ligne est exposée à l'orage, l'utilisation de para-surtenseurs est recommandée.

11 Raccordement des entrées sorties



L'entrée tout ou rien permet au routeur d'émettre une alarme par e-mail ou bien de commander la connexion du routeur à l'Internet.

Par ailleurs, le menu du menu « Contrôle des E/S » du routeur d'administration permet de visualiser l'état de l'entré et de télécommander la sortie.

12 Raccordement au réseau cellulaire

12.1 Contrôles avant installation

Autorisation d'utilisation
Si le routeur doit être installé en dehors du domaine public, comme par exemple sur un aéroport ou une zone militaire, usine de production … on vérifiera auprès de la personne habilitée que l'utilisation d'un routeur cellulaire est autorisée

Contrôle préalable du niveau de réception au moyen des cartes de couverture des opérateurs
Les cartes de couverture de réseau publiées par les opérateurs sur l'Internet permettent de vérifier grossièrement la disponibilité du service sur le lieu ou l'installation du routeur est envisagée.

La consultation des cartes de couverture permet de choisir l'opérateur télécom le plus adapté.

Contrôle de la réception sur site
Si la réception semble possible après avoir consulté la carte de couverture, il est utile de confirmer la faisabilité sur le site lui-même.

Le contrôle doit être effectué à l'emplacement où il est prévu d'installer le routeur, tout particulièrement dans le cas où il doit être installé en ville et/ou à l'intérieur d'un bâtiment.

Le contrôle doit être effectué en utilisant le même opérateur de réseau cellulaire que celui qui est prévu pour le routeur.

Une bonne solution, si le routeur n'a pas encore été commandé ou livré, est de réaliser le test au moyen d'un smartphone ; les menus « paramètres » ou « diagnostic » de tous les smartphones permettent d'afficher le niveau de réception.

Il est également possible d'utiliser le routeur IPL-C ; le voyant de niveau de champ et le menu diagnostic permettent d'afficher le niveau de réception.

12.2 Antenne

L'antenne est fournie séparément.

Si l'armoire dans laquelle doit être installé le routeur est en matériau synthétique et que le niveau de réception est bon, l'antenne peut être fixée directement sur le routeur (ANT210).

Autrement, nous proposons un catalogue d'antennes permettant les installations dans les cas les plus variés :
Antenne magnétique (ANT211).
Antenne de traversée de cloison à fixer sur le dessus d'une armoire (ANT210).
Antenne disque à plan de masse intégré (ANT214).
Antenne directive (conseillée uniquement lorsque le niveau de réception est médiocre).
Antenne mât pour installation sur un toît ou contre un mur.

12.3 Déport de l'antenne

L'antenne peut être déportée ; cependant, le câble coaxial absorbe le signal reçu ou émis.

Si l'on utilise un câble de diamètre 6 mm, le niveau de réception du signal est diminué de 0,4 dB par mètre soit 4 dB environ tous les 10 mètres; on veillera à ce que le rallonge ne dégrade pas le signal en dessous de la valeur minimale requise pour une connexion fiable (- 90 dBm).

On peut aussi utiliser du câble coaxial de diamètre 10 mm environ pour diminuer la perte dans le câble (0,2dB/m au lieu de 0,4dB/m).

Nous fournissons les rallonges à notre catalogue.

12.4 Choix de l'abonnement au réseau cellulaire

Un abonnement autorisant la transmission de données 4G-3G ou GPRS-EDGE doit être souscrit.
On pourra choisir, par exemple, un abonnement fait pour les tablettes ou pour les sticks USB
Il est inutile de souscrire un abonnement autorisant la téléphonie.

On choisira un abonnement qui autorise un volume mensuel suffisant au regard de l'application envisagée.

On vérifiera le coût du MO supplémentaire transmis au-delà du volume mensuel forfaitaire.

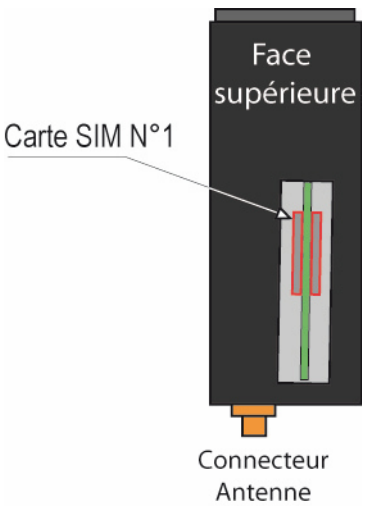
On souscrira de préférence l'abonnement dans le pays où le routeur doit être installé afin d'éviter les sur-coûts de « roaming ».
Par exemple, si le routeur doit être installé en Suède, on souscrira l'abonnement auprès d'un opérateur en Suède.

12.5 Installation ou extraction de la carte SIM (ou des 2 cartes SIM)

Le routeur permet l'installation de 1 ou 2 cartes SIM.

Les porte-cartes SIM situés sous la trappe de protection de la face supérieure du produit.

Pour les systèmes critiques, 2 cartes SIM provenant du même opérateur ou de 2 opérateurs différents peuvent être utilisées.



Remarque :
Pour mettre le produit en service, le code PIN de la carte et l'APN doivent être saisis (Libellé de la passerelle vers Internet ou un réseau privé du réseau d'opérateur; voir chapitre « Mise en service »).

Installation de la carte SIM

Placer le routeur hors tension.

Dégager la trappe située sur la face supérieure.

Insérer la carte SIM dans l'un des 2 porte-cartes ; <u>la puce de la carte SIM doit être face au circuit imprimé (voir schéma).</u>

Pousser la carte jusqu'à ce qu'elle se verrouille.

Extraction de la carte SIM

Placer le routeur hors tension.
Dégager la trappe située sur la face supérieure.
Appuyer sur la carte SIM pour la déverrouiller ; elle remonte de quelques millimètres afin de faciliter son extraction.

12.6 Contrôle de la conformité de la connexion

Après installation, il est conseillé de vérifier la conformité du fonctionnement de la liaison avec le réseau cellulaire.

Si la connexion n'est pas conforme, il faut impérativement améliorer les conditions de réception pour rendre la connexion fiable soit en modifiant le type ou la position de l'antenne, soit en sélectionnant un autre réseau : 3G, voire GPRS, par exemple, au lieu de 4G.

La conformité de la liaison se mesure au moyen des paramètres suivants :

- Niveau de réception :

Voyant de réception du signal cellulaire		
Description	**Status**	**Niveau de réception dBm (*)**
3 flashs	<u>Bonne réception</u> Le routeur capte le réseau; le niveau de réception est bon.	-50 à - 80
2 flashs	<u>Réception suffisante</u> Le routeur capte le réseau ; le niveau de réception est suffisant pour assurer une liaison fiable. Cependant, le débit pourra être diminué en cas d'erreurs de transmission.	-81 à –90
1 flash	<u>Réception insuffisante</u> Le routeur capte le réseau. Le niveau de réception est faible ; des déconnexions plus ou moins fréquentes et des erreurs peuvent survenir. Il faut améliorer la réception.	-91 à -110
Eteint	<u>Pas de réception</u> Contrôler le connecteur d'antenne et la présence de la carte SIM.	< -111

Remarque : On peut contrôler en permanence le niveau du signal de réception au moyen du serveur html dans le menu Diagnostic > Etat réseau > Interface.

1 Etapes de la configuration du routeur

Pour configurer le routeur, nous conseillons de procéder comme suit :

- Connecter un PC au routeur
- Configurer la connexion cellulaire
- Configurer l'interface LAN
- Configurer les VPN avec d'autres routeurs
- Configurer les fonctions de translation d'adresse et redirection de port
- Configurer les passerelles série
- Configurer la connexion d'utilisateur distant et la liste des utilisateurs distants
- Configurer le firewall

2 Introduction en vue de la configuration

Première configuration
La première configuration s'effectue au moyen d'un navigateur HTML et en connectant le PC directement à l'un des connecteurs Ethernet de l'interface LAN du produit.

Les modifications ultérieures peuvent être en plus effectuées depuis le réseau LAN, ou bien à distance si cette possibilité est autorisée.

Modes de configuration
Le routeur se configure par l'un des moyens suivants :

- Au moyen d'un navigateur HTML avec le protocole HTTP
- Au moyen d'un navigateur HTML avec le protocole de sécurité HTTPS
- En mode commande, au moyen d'une connexion sécurisée SSH

Adresse du serveur de configuration
Le serveur de configuration se trouve à l'adresse IP attribuée à l'interface LAN du routeur (= adresse IP attribuée au switch Ethernet 2 ou 4 ports).

A la livraison, l'adresse attribuée à l'interface LAN est 192.168.0.128.

Choix du navigateur HTML
L'interface web a été validée avec Mozilla Firefox, Google Chrome et Internet Explorer 7 et plus.

Res**titution de l'adresse IP Usine et suspension provisoire de la sécurité d'accès au serveur de configuration**
L'accès non sécurisé au serveur de configuration, sans mot de passe et à l'adresse IP Usine 192.168.0.128 est restitué en pressant le poussoir situé à l'arrière du produit. La configuration courante est conservée.

Format des adresses réseau
Dans la suite du texte on appelle « adresse réseau », l'adresse de valeur la plus basse du réseau.

Par exemple si le netmask est 255.255.255.0, l'adresse réseau est X.Y.Z.0.

Caractères autorisés
les caractères accentués ne peuvent être saisis.

Sauvegarde de la configuration
Il est conseillé de sauvegarder la configuration du routeur dans un fichier.

3 Configuration au moyen d'un navigateur en HTTP

HTTP est le protocole de transmission des pages HTML.
C'est le mode de configuration de base du routeur.

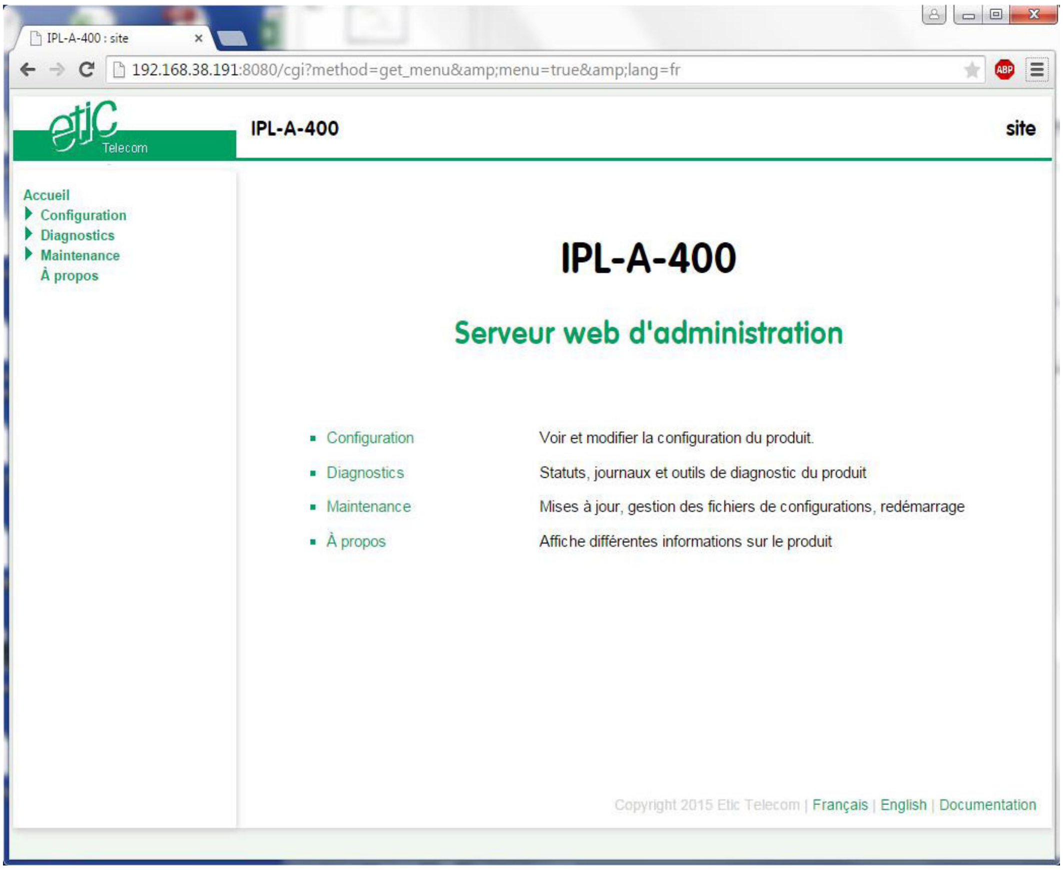
3.1 Première configuration

Etape 1 : Créer ou modifier la connexion TCP/IP du PC (voir annexe 1).
Attribuer à cette connexion une adresse IP différente mais cohérente avec l'adresse IP usine du routeur qui est 192.168.0.128.
On utilisera par exemple l'adresse 192.168.0.127 pour le PC.

Etape 2 : Connecter le PC au routeur
Connecter le PC au routeur.

Etape 3 : Lancer le navigateur HTML
Ouvrir le navigateur, effacer l'historique, et saisir l'adresse IP du serveur d'administration programmée en usine : 192.168.0.128 (ne pas faire précéder l'adresse de www).

La page d'accueil du serveur d'administration s'affiche.



3.2 Protection de l'accès au serveur d'administration

L'accès en http au serveur d'administration peut être protégé :

- Sélectionner le menu « **Configuration** », « **Sécurité** » puis « **Droits d'administration** ».

Saisir le nom d'utilisateur et le mot de passe qui protègent l'accès au serveur d'administration.

4 Configuration au moyen d'un navigateur en HTTPS

Le protocole HTTPS permet de transporter en particulier les pages HTML en authentifiant l'utilisateur et en cryptant les données.

4.1 Sélection du mode HTTPS

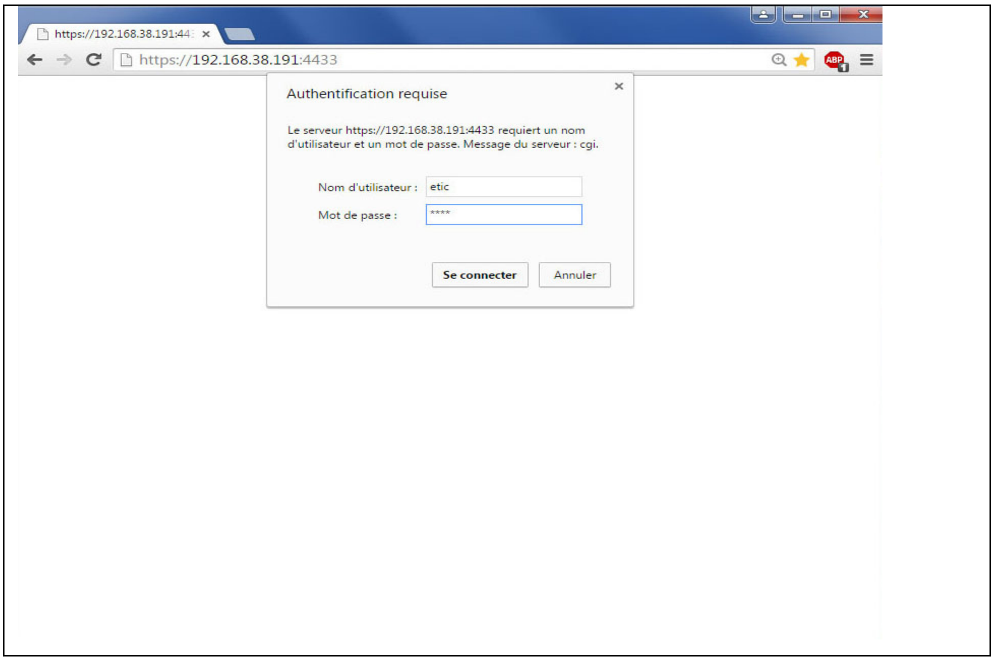
HTTPS est un protocole qui permet d'authentifier et cryptée les connexions HTML

Pour sélectionner le mode HTTPS,

- Accéder au serveur de configuration au moyen d'un navigateur HTML
- Sélectionner le menu Configuration > Sécurité >Droits d'administration
- Saisir le nom d'utilisateur et le mot de passe
- Cocher la case « utiliser HTTPS pour la configuration »
- Cocher éventuellement la case « Activer l'accès par le WAN »
- Enregistrer

4.2 Configuration en HTTPS

- Ouvrir le navigateur et saisir l'adresse IP du serveur d'administration du routeur :
- Exemple : https://192.168.38.191:4433.
- Cliquer sur « continuer » lorsque le navigateur affiche un message d'avertissement.
- Saisir le nom d'utilisateur et le mot de passe qui ont été programmés pour protéger l'accès au serveur d'administration.



La page d'accueil du serveur de configuration s'affiche.

5 Configuration en SSH

La connexion SSH (Secure Shell) est une connexion telnet sécurisée par le protocole TLS.

Le port SSH est 22

Le nom et le mot de passe permettant une connexion SSH sont ceux qui ont été configurés dans la page web "Droits d'administration".

L'utilisateur peut alors consulter ou modifier les paramètres de configuration en mode « commande CLI ».

6 Modification de la configuration à distance

Par défaut, l'accès à la configuration à distance par le port WAN n'est pas autorisé.

Pour autoriser la configuration à distance par le réseau cellulaire ou par le port Ethernet N°1 s'il a été désigné comme un port WAN,

- Sélectionner le menu Configuration > Sécurité >Droits d'administration
- Cocher la case « Activer l'accès par le WAN »
- Enregistrer

7 Restituer l'@IP Usine et l'accès libre à l'administration

- Appuyer sur le bouton-poussoir placé sur la face arrière du produit ; la led d'alimentation clignote rapidement en rouge.

Le routeur reprend l'adresse IP usine 192.168.0.128 jusqu'à la prochaine mise sous tension.

Le serveur HTML d'administration est accessible sans mot de passe et en HTTP jusqu'à la prochaine mise sous tension.

<u>La configuration programmée n'est pas modifiée.</u>

Remarque :
Le logiciel ETICFinder permet de détecter tous les produits fabriqués par ETIC TELECOM et connectés à un réseau Ethernet ; le logiciel affiche l'adresse IP attribuée à chacun d'entre eux.

8 Retour à la configuration Usine

Il peut être nécessaire de restaurer la configuration Usine, par exemple, si l'accès au serveur d'administration n'est plus possible à la suite d'une erreur dans la programmation du firewall ou bien pour d'autres raisons.

Il est possible de de restituer la configuration Usine au moyen du bouton poussoir de la face arrière, ou bien en utilisant le serveur d'administration.

Pour restituer la configuration Usine au moyen du bouton poussoir de la face arrière du routeur,

- Mettre le routeur hors tension,
- Retirer le routeur de son rail DIN.
- Appuyer sur le poussoir de la face arrière avec une pointe de tournevis par exemple.
- Mettre sous en tension tout en maintenant le poussoir enfoncé.

Le voyant « Service » passe au rouge ; le routeur s'initialise et la configuration Usine est restituée.

Pour restituer la configuration Usine au moyen du serveur d'administration,

- Sélectionner le menu « Maintenance », puis le menu « Gestion des configurations ».
- Sélectionner la configuration « Factorydefault » puis cliquer le bouton « charger ».

Le voyant « Operations » passe au rouge ; le routeur s'initialise et la configuration par défaut est restituée.

Remarque :
Après avoir restauré la configuration Usine du routeur, la configuration courante est perdue, sauf si elle a été sauvegardée dans un fichier (voir paragraphe sauvegarde de la configuration).

9 Configuration de l'interface WAN

9.1 Principe

L'interface WAN est l'interface vers un réseau distant, c'est normalement le modem cellulaire.

Cependant, pour permettre une utilisation plus étendue du routeur, le modem cellulaire peut être remplacé par les interfaces suivants :

- L'interface Ethernet 10/100 BT de la prise RJ45 N°1 du routeur,
- ou encore l'interface WiFi.

Lors que l'interface Ethernet de la prise RJ45 N°1 ou bien l'interface WiFi sont sélectionnés pour remplacer le modem cellulaire, ils jouent le même rôle que le modem cellulaire.

En particulier,

- Le VPN éventuel est établi à travers l' interface sélectionnée (Ethernet ou WiFi) au lieu de l'interface cellulaire,
- Les fonctions de redirection de port sont effectuées entre l'interface sélectionnée et l'interface LAN,
- le firewall joue son rôle entre l'interface sélectionnée et l'interface LAN,
- les utilisateurs distants sont accueillis sur l'interface sélectionnée (Ethernet ou WiFi),

On décrit ci-dessous successivement la configuration de l'interface WAN du routeur lorsque le modem cellulaire ou l'interface WiFi ou le port Ethernet N°1 sont sélectionnés.

9.2 Configuration de l'interface WAN / cellulaire

Deux cartes SIM peuvent être insérées dans le routeur pour permettre l'utilisation d'un deuxième réseau cellulaire en cas de panne du premier.

- Sélectionner le menu Configuration > Interface WAN

Case à cocher « Type de WAN » :
Choisir la valeur « Cellulaire».

Paramètre « Priorité » :
Le paramètre « priorité » permet de hiérarchiser la priorité entre plusieurs routes pouvant agir en secours l'une de l'autre. En l'absence de route de secours, saisir la valeur 10.

Remarque : plus la valeur est élevée (1 à 100) mois la route est prioritaire.

Paramètre « Carte SIM » :
Il est possible de sélectionner la carte SIM N°1, ou bien la carte SIM N°2, ou bien les deux.

Paramètre carte SIM	
Valeur	
SIM1	La carte SIM placée dans le logement 1 est sélectionnée
SIM2	La carte SIM placée dans le logement 2 est sélectionnée
SIM 1, backup sur SIM2	Le routeur utilise la carte SIM N°1en priorité et, en cas de défaut de fonctionnement du réseau cellulaire, il utilise la carte SIM2 Dans ce cas, les temporisations de asculement d'un résau à l'autre doivent être réglées.

9.2.1 Configuration de la carte SIM 1 ou de la carte SIM2

On décrit ci-dessous la configuration de la carte SIM du logement 1.

La configuration de la carte SIM du logement 2 est identique.

Paragraphe « SIM1 : Configuration du modem »

Paramètre « Chaîne d'initiatlisation du modem » :

Ce paramètre permet de modifier, dans des cas particulier, la chaîne d'initialisation transmise par le routeur à son modem cellulaire.
Laisser ce champ vide sauf indication de la hotline.

Paramètre « Nom du point d'accès (APN) » :
Le réseau cellulaire est connecté à d'autre réseaux, l'internet ou un réseau privé, au travers d'une passerelle appelée APN.
La ou les passerelles utilisables doivent être désignées par l'opérateur Télécom dans le contrat d'abonnement. Dans le cas contraire, on peut se reporter au site we de l'opérateur.
Entrer le nom de l'APN associé à la carte SIM (par exmple websfr ou orange business).

Paramètre « Code PIN » :
Saisir le coe PIN de la carte SIM.

Paramètre « Type de réseau cellulaire » :
Les infrastructures (c'est-à-dire les relais) 4G, 3G et GPRS sont différentes les unes des autres.
Ce paramètre permet de forcer le routeur à utiliser une de ces 3 infrastructures.

Paramètre « Type de réseau cellulaire »	
Valeur	
Auto	Si la valeur « Auto » est sélectionnée, le routeur choisit le relais qui assure la meilleure efficacité de transmission (valeur par défaut).
4G	S'il est nécessaire de forcer l'utilisation du réseau 4G, sélectionner la valeur 4G
3G	Idem
GPRS	Idem

Paragraphe « SIM1 : Configuration IP du WAN cellulaire »

Paramètres «login» et « Password» :
Saisir l'identificateur et le mot de passe du compte Internet.
Remarque sur les réseaux cellulaires, il n'est habituellement pas nécessaire de saisir ces paramètres.

Case à cocher « Obtenir une adresse IP automatiquement » :
Ce champ dot être laissé vide sauf dans le cas où une adresse IP fixe est attribuée au routeur IPL sur le réseau cellulaire.

Case à cocher « Obtenir les adresses des serveurs DNS automatiquement» :
Cocher cette case si l'adresse des serveurs DNS est attribuée par l'opérateur à travers la ligne.

Case à cocher « Translation d'adresse NAT»:
Cocher cette case pour que le routeur ETIC substitue son adresse IP publique à l'adresse IP source de l'équipement du réseau LAN lors d'une transaction vers l'Internet.

9.2.2 Cas où deux cartes SIM sont utilisées en secours l'une de l'autre

Le routeur IPL-C comporte deux logements pour carte SIM.

Chaque carte SIM peut être associée à un abonnement différent ; l'un chez un opérateur et l'autre chez un autre opérateur.

Dans la suite du texte, on nomme « réseau 1 » le réseau cellulaire associé à la carte SIM N°1, et « réseau 2 » le réseau associé à la carte SIM N°2.

Le réseau 1 est le réseau testé à la mise sous tension du routeur.

En cas de défaillance du réseau 1 confirmée durant le temps T1, le routeur bascule sur le réseau 2.
Si le réseau 2 fonctionne correctement, le routeur y reste au minimum pendant le temps T3 ; à l'issue de ce temps, le routeur interrompt la communication sur le réseau 2, teste le réseau 1 et retourne sur le réseau 1 s'il est à nouveau disponible.

A tout moment, si le réseau 2 ne fonctionne pas correctement et après confirmation pendant le temps T2, le routeur retourne sur le réseau 1.

Les temporisations T1, T2 et T3 peuvent être réglées.

Paramètre T1 «Temps avant basculement sur SIM2» :
Saisir le temps de confirmation d'indisponibilité du réseau 1 au-delà duquel le routeur bascule sur le réseau 2.
Valeur : 5, 10, 20, 30, 60 mn

Paramètre T2 «Temps avant re-basculement sur SIM1» :
Saisir temps de confirmation d'indisponibilité du réseau 2 au-delà duquel le routeur bascule sur le réseau 1.
Valeur : 2, 5, 10, 20 mn

Paramètre T3 «Temps de connexion sur SIM2 avant de re-tester SIM1» :
Saisir le temps minimum durant lequel le routeur demeure sur le réseau 2, s'il fonctionne correctement.
Valeur : 1, 12, 24 heures, 5 jours, jamais

Remarque :
Il est conseillé de donner à T3 une valeur longue (12 heures par exemple); en effet, si le réseau 2 fonctionne correctement, il n'est pas nécessaire de retourner immédiatement sur le réseau 1.

9.2.3 Configuration du contrôle de la connexion cellulaire

Le routeur contrôle la connexion au réseau cellulaire en testant le fonctionnement de la connexion PPP au serveur de l'opérateur du réseau cellulaire. Cette technique est la technique normale de vérification du fonctionnement de la liaison.

Cependant, il a été constaté que, sur certains réseaux ou à certains moments, la connexion PPP pouvait être déclarée active alors que le service de transmission de données n'était pas rendu par l'opérateur de réseau cellulaire.

C'est la raison pour laquelle le routeur IPL-C peut vérifier le fonctionnement du service en transmettant un message ICMP (PING) vers un serveur distant.

Si le message n'obtient pas de réponse, et après réitération, le routeur initialise son module de transmission de données 4G / 3G.

Cette fonction ne doit être activée que si un dysfonctionnement est constaté.

Paramètre «Adresse IP du serveur» :
Saisir l'adresse IP du serveur vers lequel le message ICMP (PING) doit être transmis.

Paramètre «Intervalle des PING» :
Saisir la période de transmission des PING

Paramètre «Nombre d'essais» :
Saisir le nombre de tests infructueux successifs avant de réinitialiser le module de transmission de données 4G / 3G.

9.3 Configuration de l'interface WAN / Ethernet

L'interface WAN normalement sélectionné est l'interface cellulaire dont la configuration a été décrite au paragraphe précédent.
Cependant, il peut être utile d'utiliser l'interface Ethernet de la RJ45 N°1 au lieu de l'interface cellulaire, par exemple pour utiliser un accès existant à l'internet.

Pour sélectionner l'interface Ethernet à la place de l'interface cellulaire,

- Sélectionner le menu Configuration > Interface WAN

Case à cocher « Type de WAN » :
Choisir la valeur « Ethernet» pour désigner le port Ethernet N°1 comme interface WAN.

Paragraphe « Configuration du WAN Ethernet »

Paramètre « Speed / Duplex» :
CSélectioner 10 ou 100 Mb/s et full ou half duplex.

Paragraphe « Configuration IP du WAN Ethernet »

Case à cocher « Activer » :
Sélectionner la case à cocher

Case à cocher « PPPoE » :
PPPoE assure l'établissement d'une connexion PPP (point to point protocol) entre le port Ethernet N°1 du routeur IPL et un fournisseur de service (FAI) sur l'internet via un modem connecté au port Ethernet du routeur IPL.

Cette solution permet à l'interface Ethernet du routeur IPL de recevoir une adresse IP publique de l'Internet ce qui peut être utile lorsque l'on utilise IPSec par exemple, ou que l'on souhaite mettre en œuvre des fonctions de redirection de port.

Ne pas sélectionner cette case, sauf dans le cas très particulier décrit ci-dessus.

	Ethernet	Ethernet et PPPoE
Paramètre « priorité du WAN Ethernet» (valeur 0 à 100) : Saisir la valeur 10.	●	●
Paramètres « PPP login» et « mot de passe PPP »: Saisir l'identificateur et le mot de passe du compte Internet.		●
Case à cocher « Obtenir une adresse IP automatiquement »: Cocher cette case si l'adresse IP de la ligne est attribuée par l'opérateur à travers la ligne. Autrement, décocher cette case et saisir l'adresse IP attribuée au routeur ETIC ainsi que celle du serveur distant.	●	
Case à cocher « Obtenir les adresses des serveurs DNS automatiquement»: Cocher cette case si l'adresse des serveurs DNS est attribuée par l'opérateur à travers la ligne. Autrement, décocher cette case et saisir l'adresse IP des serveurs DNS primaires et secondaires.	●	●
Case à cocher « Translation d'adresse NAT»: Cocher cette case pour que le routeur ETIC substitue son adresse IP publique à l'adresse IP source de l'équipement du réseau LAN lors d'une transaction vers l'Internet.	●	●
Case à cocher « Activer le Proxy-Arp »: Cette fonction permet de rendre l'équipement distant (BRAS / broadband remote access server) accessible depuis le LAN. Laisser cette case désactivée sauf sur demande de la hotline.	●	●

9.4 Configuration de l'interface WAN / WiFi

L'interface WAN normalement sélectionné est l'interface cellulaire dont la configuration a été décrite au paragraphe précédent.

Cependant, il peut être utile d'utiliser l'interface WiFi au lieu de l'interface cellulaire.

Dans ce cas, l'interface WiFi du routeur IPL est un client WiFi (et pas un point d'accès).

Lorsque l'interface WiFi est sélectionnée comme interface WAN, le voyant WiFi s'éclaire et le voyant de niveau de réception indique la qualité de la liaison avec le point d'accès.

Pour sélectionner l'interface WiFi à la place de l'interface cellulaire,

- Sélectionner le menu Configuration > Interface WAN
- Sélectionner le type de WAN « WiFi »

Paramètre « Nom de réseau WiFi (SSID) » :
Saisir un libellé libre qui désigne le réseau WiFi.

Paramètre « Authentification » :
Choisir le mode d'authentification WPA ou WEP ou le mode non sécurisé (non recommandé).

Paramètre « Clé partagée » :
Saisir la clé WPA ou WEP du réseau.
Elle est fixée par le point d'accès WiFi.

Paramètre « Priorité du WAN WiFi» :
Saisir la valeur 10.

Case à cocher « Obtenir une adresse IP automatiquement »:
Cocher cette case si l'adresse IP est attribuée par le point d'accès WiFi.

Autrement, décocher cette case et saisir l'adresse IP attribuée au routeur ETIC sur cette interface, le masque de sous-réseau et l'adresse IP de la passerelle par défaut.

Case à cocher « Obtenir les adresses des serveurs DNS automatiquement»:
Cocher cette case si l'adresse des serveurs DNS est attribuée par le point d'accès WiFi..

Autrement, décocher cette case et saisir l'adresse IP des serveurs DNS primaires et secondaires.

Case à cocher « Translation d'adresse NAT»:
Cocher cette case pour que le routeur ETIC substitue l'adresse IP qui lui a été attribuée sur le réseau WiFI à l'adresse IP source de l'équipement du réseau LAN lors des transactions sur le réseau WiFi

Remarque :
Le scanner WiFi du router IPL permet d'identifier les réseaux WiFi détectés par le routeur.
Pour utiliser le scanner WiFi, sélectionner le menu Diagnostic > Outils > Scan WiFi.
(Voir le chapitre Diagnostic de la présente notice).

10 Interface LAN

10.1 Principes de configuration

Switch Ethernet
L'interface LAN est constituée de 2 ou 4 prises Ethernet switchées.
Cette interface est désignée par « interface LAN » dans la suite du texte ; et le réseau qui y est directement raccordé est appelé « réseau LAN ».
Les ports Ethernet peuvent être paramétrés pour former un hub au lieu d'un switch.

Adresse IP du routeur sur l'interface LAN
Une adresse IP fixe doit être attribuée à l'interface LAN du routeur.

Serveur DHCP
Le routeur peut être serveur DHCP pour les équipements du réseau local (LAN).

Réserve d'adresses pour les utilisateurs distants
Si le routeur est aussi utilisé pour permettre à des utilisateurs distants d'échanger des données avec les équipements du réseau local au moyen d'une connexion distante (PPTP ou TLS ou L2TP) , une plage d'adresses IP du réseau local doit leur être réservée.
Les adresses de cette plage ne doivent donc pas être attribuées aux équipements du réseau local.

<u>Exemple :</u>

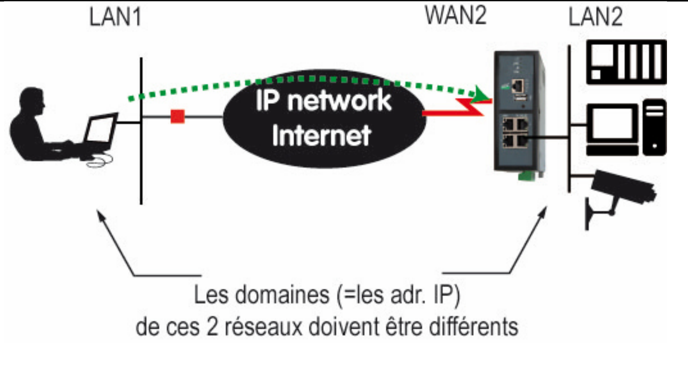
<table>
<tr><td>Désignation</td><td>Adresse IP</td><td>Observations</td></tr>
<tr><td>Réseau LAN</td><td>192.168.12.0</td><td>Les adr. des équipements du réseau vont de 192.168.12.1 à 192.168.12.254</td></tr>
<tr><td>Netmask</td><td>255.255.255.0</td><td></td></tr>
<tr><td>Interface LAN Routeur ETIC</td><td>192.168.12.1</td><td>L'adr IP du routeur ETIC sur le réseau LAN est 192.168.12.1</td></tr>
<tr><td>Début de plage utilisateurs distants</td><td>192.168.12.2</td><td rowspan="2">2 utilisateurs distants pourront se connecter simultanément au réseau LAN.
L'un recevra l'adresse 192.168.12.2 et l'autre 192.168.12.3.
Ces 2 adresses ne peuvent pas être attribuées à d'autres équipements du réseau LAN</td></tr>
<tr><td>Fin de plage utilisateurs distants</td><td>192.168.12.3</td></tr>
<tr><td>Adresses disponibles pour les équipements du réseau local</td><td>192.168.12.4 à
192.168.12.254</td><td></td></tr>
</table>

Nom des équipements raccordés au réseau LAN
Il est possible d'attribuer un nom à chaque équipement ou groupe d'équipements connectés à l'interface LAN.
Ce nom permet ensuite de d »finir els droits d'accès des utilisateurs distants.

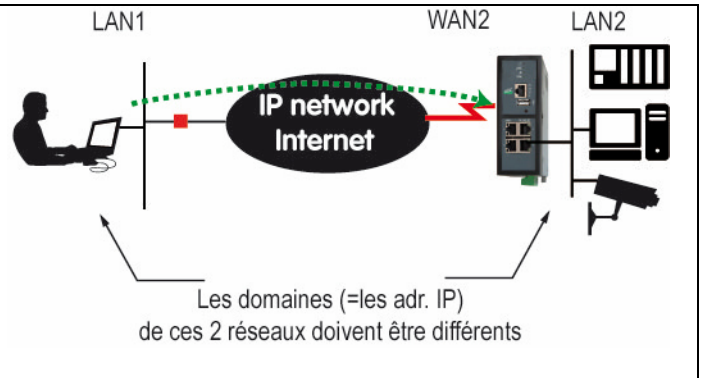
Interface WiFi optionnelle
L'interface WiFi optionnelle vient compléter l'interface LAN lorsqu'elle est configurée en « Point d'accès ».
Les équipements qui se connectent en Wifi appartiennent au réseau LAN.
En particulier, les adresses IP de ces équipements font partie du domaine IP du réseau LAN.

Règles d'attribution de l'adresse IP de l'interface LAN

Cas d'une connexion distante
Le plan d'adresses IP du réseau du PC distant d'une part, et du réseau LAN d'autre part, doivent être disjoints.



Cas d'un VPN établi avec un autre routeur
Le plan d'adresses IP du réseau distant d'une part, et du réseau LAN d'autre part, doivent être disjoints.



10.2 Menu Ethernet et IP

- Sélectionner le menu Configuration > Interface LAN > Ethernet & IP

10.2.1 Paramètres « Ports Ethernet »

Case à cocher « Activer le mode hub » :
Si cette case est cochée, le switch Ethernet devient un hub ; les trames Ethernet sont diffusées sur tous les ports.

10.2.2 Paramètres « Réseau LAN »

Paramètre « Adresse IP » :
Saisir l'adresse IP attribuée à l'interface LAN du routeur.

Paramètre « Masque de sous-réseau » (netmask) :
Saisir le netmask du réseau LAN.
Exemple : Le netmask d'un réseau de 254 stations est 255.255.255.0.

Paramètre « Passerelle par défaut » :
S'il un autre routeur est raccordé au réseau LAN et si ce routeur est le routeur par défaut du routeur ETIC, saisir son adresse. Cette adresse doit faire partie du domaine du réseau LAN.

Remarque : Ne rien saisir si aucun autre routeur n'est connecté au réseau LAN

10.2.3 Paramètres « Accès distant »

Case à cocher « Gestion automatique des adresses IP des utilisateurs distants » :
Si cette case est cochée, une adresse IP non utilisée du réseau LAN est attribuée au PC d'un utilisateur distant lorsqu'il se connecte.

Pour attribuer cette adresse, le routeur ETIC vérifie au moyen de requêtes appropriées qu'elle n'est pas attribuée par ailleurs à un équipement du réseau LAN.

Décocher la case pour fixer la plage des adresses du réseau LAN réservée aux utilisateurs distants.

Remarque : La plage doit comporter autant d'adresses que l'on souhaite d'accès simultanés.

Paramètre « Début de la plage d'adresses IP » :
Saisir l'adresse IP du début de la plage

Paramètre « Fin de la plage d'adresses IP » :
Saisir l'adresse IP de la fin de la plage

10.2.4 Paramètres « Paramètres avancés »

Pour afficher ces paramètres, cocher la case « paramètres avancés ».

Paramètres « Configuration port 1 » à « Configuration port 4 »:
Les ports 1 à 4 (ou 1 à 2) du switch Ethernet sont à détection automatique de débit ; cependant, dans des cas particuliers, il peut être utile de fixer leur comportement ou encore de désactiver certains ports pour des raisons de sécurité.

Valeur	Observation
Auto-négociation	Le switch négocie le débit et le mode de fonctionnement du port Ethernet
100 M full duplex	
10 M full duplex	
100 M half duplex	
10 M half duplex	
Désactivé	Le fonctionnement du port Ethernet est désactivé

Paramètre « Serveur DNS primaire » :
Saisir l'adresse P du serveur DNS principal.

Paramètre « Serveur DNS secondaire » :
Saisir l'adresse P du serveur DNS secondaire.

Case à cocher « Activer proxy ARP » :
Proxy-Arp permet au routeur de simuler sur son interface LAN le comportement d'un équipement situé sur son interface WAN afin que les trames IP puissent effectivement être routées du LAN vers le WAN.

Cette fonction peut être nécessaire, par exemple, lorsque des équipements possédant une adresse IP du domaine du LAN, sont connectés à l'interface WAN.

Cette fonction n'est pas nécessaire habituellement.

Paramètre « Adresse IP additionnelle » et « Masque de sous-réseau additionnel » :
Il est possible d'attribuer une seconde adresse IP à l'interface LAN du routeur.
Dans ce cas, le routeur appartient aux deux réseaux IP.

Case à cocher « Désactiver ICMP redirect » :
ICMP est un protocole de même niveau que IP.
Il permet aux équipements de gérer les erreurs survenant sur le réseau.
ICMP redirect est un des messages de ICMP.
Lorsque plusieurs routeurs sont présents sur l'interface LAN, et qu'un équipement fait appel à tort au routeur IPL pour router les trames IP vers un autre réseau, « ICMP redirect » permet au routeur IPL de transmettre à cet équipement la route adaptée (c'est-à-dire l'adresse IP d'un autre routeur du réseau LAN).

10.3 Menu « Serveur DHCP »

La fonction serveur DHCP permet de réserver une plage d'adresses IP du domaine du réseau LAN.
Les adresses de cette plage sont automatiquement attribuées aux équipements du réseau LAN configurés en client DHCP lorsqu'ils en font la demande.

Les adresses extérieures à cette plage peuvent être attribuées de manière fixe aux autres équipements du réseau.

Remarque :
Lorsque le routeur est équipé de l'option WiFi et qu'il est configuré en point d'accès afin de permettre la connexion d'équipements WiFi tels qu'un PC, une tablette ou un smartphone, il est conseillé de sélectionner la fonction serveur DHCP sur l'interface LAN ; en effet, de nombreux équipements de ce type ne fonctionnent que lorsqu'un serveur DHCP attribue les adresses IP.

- Sélectionner le menu Configuration > Interface LAN > Serveur DHCP

Case à cocher «Activer le serveur» :
Si cette case est cochée, le routeur se comporte en serveur DHCP sur l'interface LAN.

Paramètre « Début de la plage d'adresses IP » :
Saisir l'adresse IP du début de la plage que le routeur peut attribuer aux équipements du réseau LAN.

Paramètre « Fin de la plage d'adresses IP » :
Saisir l'adresse IP de la fin de la plage que le routeur peut attribuer aux équipements du réseau LAN.

Remarque : Lorsque le routeur possède l'option WiFi et que l'interface Wifi est configurée en point d'accès, il est conseillé

Paramètre « Masque de sous-réseau » :
Saisir le masque du réseau LAN

Paramètre « Passerelle par défaut » :
Saisir l'adresse IP de la passerelle par défaut sur l'interface LAN (s'il en existe une).

Paramètre « Serveur DNS primaire » :
Saisir l'adresse IP du serveur DNS secondaire.

Paramètre « Serveur DNS secondaire » :
Saisir l'adresse IP du serveur DNS secondaire.

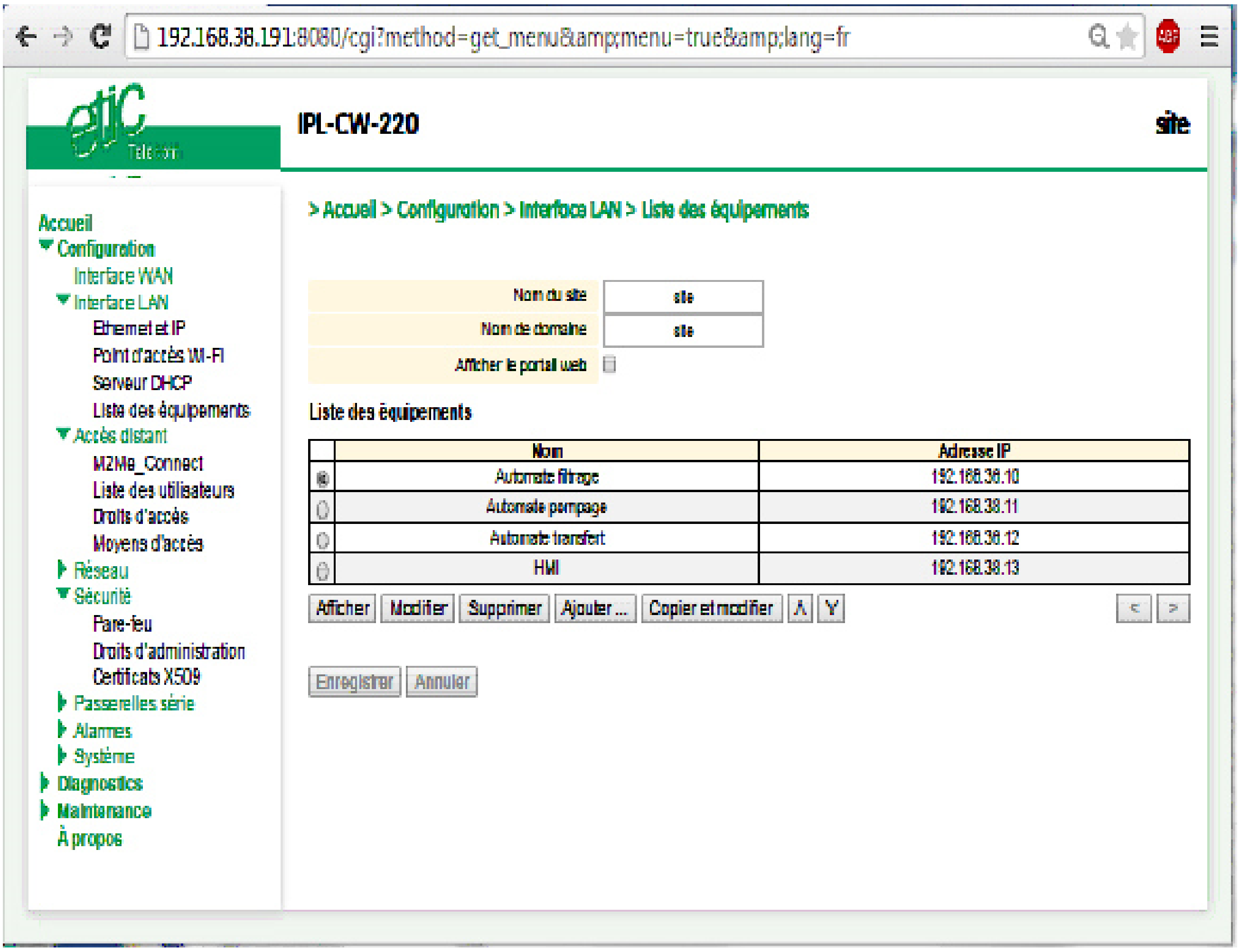
Remarque : les 4 paramètres ci-dessus sont les mêmes que ceux qui ont été saisis préalablement (menu Ethernet et IP) ; ils doivent être saisis à nouveau si le serveur DHCP est utilisé.

10.4 Menu « Liste des équipements »

Cette page permet de désigner par un nom et une adresse IP les équipements connectés au réseau LAN.

Il est nécessaire de désigner les équipements du réseau LAN qui doivent être rendus sélectivement accessibles aux utilisateurs distants.

- Sélectionner le menu Configuration > Interface LAN > Liste des équipements



Pour désigner un équipement du réseau :

- Cliquer le bouton « Ajouter »,
- Attribuer un nom et une adresse IP du réseau LAN à l'équipement.

Remarque : On peut aussi attribuer à un équipement un nom et un ensemble d'adresse IP appartenant au même sous réseau.

Exemple : 192.168.38.8/29 pour désigner la plage d'adresses IP allant de 192.168.38.8 à 192.168.38.15

10.5 Menu « Point d'accès WiFi »

L'interface WiFi (optionnel) peut être configuré comme point d'accès ou bien comme client WiFi.

Ce menu permet de configurer l'interface WiFi lorsqu'il est utilisé en point d'accès.

Pour configurer l'interface WiFi en point d'accès,

- Sélectionner le menu Configuration > Interface LAN > Point d'accès WiFi.
- Cocher la case Activer le point d'accès WiFi.

Paramètre « Nom de réseau WiFi (SSID) » :
Saisir un libellé libre qui désigne le réseau WiFi.

Paramètre « Clé partagée WPA » :
Saisir la clé WPA du réseau ; elle doit comporter au moins 8 caractères.

Remarque : Cette clé doit également être saisie dans les équipements WiFi raccordés au point d'accès.

Paramètre « Code Pays» :
l'interface WiFi du routeur IPL peut être utilisé dans différents pays.
Cependant, les canaux WiFi autorisés peuvent être différents d'un pays à un autre.
C'est pour cette raison qu'il est impératif d'indiquer le pays dans lequel est utilisé le routeur.

Saisir le code du pays selon la syntaxe de l'annexe 2.

Paramètre « Mode» :
Les canaux radio-fréquences utilisés associés à la technologie de transmission forment les modes de fonctionnement du réseau WiFi.

Trois modes de fonctionnement sont proposés :

Mode 802.11a : 5 GHz OFDM
Mode 802.11.b : 2,4 GHz DSSS
Mode 802.11.g : 2,4 GHz OFDM

Remarque : Le mode choisi doit également être attribué au client WiFi.

Case à cocher « Activer 802.11n haut débit » :
Le mode 802.11n permet de transmettre à un débit plus élevé (jusqu'à 200 Mb/s) mais avec une portée réduite : 100 mètres en champ libre et au maximum.

Remarque :
Si ce mode est sélectionné, il est nécessaire de s'assurer du fonctionnement avec les clients WiFi envisagé et dans la zone envisagée.

Paramètre « canal» :
Le point d'accès WiFi peut utiliser un canal radio-fréquence parmi la liste proposée.

Il est préférable d'utiliser un canal radio non utilisé par un autre réseau WiFi de la même zone.

Le scanner Wifi permet de détecter les réseaux WiFi de la même zone (Voir le chapitre Diagnostic de la présente notice).

11 Publier l'adresse IP dynamique du routeur sur l'Internet

11.1 Principe

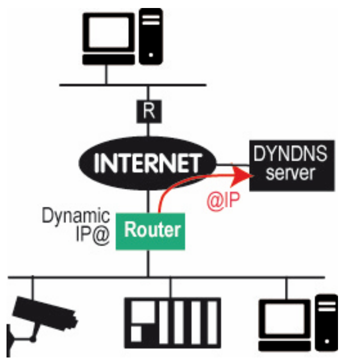
L'adresse IP attribuée à un routeur cellulaire n'est généralement pas une adresse fixe mais une adresse dynamique qui change à chaque connexion ou de façon périodique.

Cependant, si l'adresse IP attribuée au routeur IPL par l'opérateur est une adresse publique de l'internet, il est possible de joindre le routeur IPL depuis l'Internet en publiant l'adresse IP obtenue sur un serveur spécialisé tel que DynDNS ou NoIP.

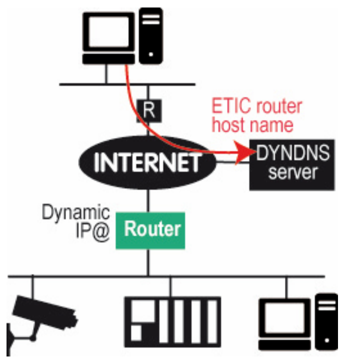
Grâce à ce type de serveur, un utilisateur pourra connecter son PC au routeur IPL en utilisant le nom de domaine dynamique enregistré auprès de DynDNS ou NoIP (mon_routeur_etictelecom.dyndns.org, par exemple) au lieu de l'adresse IP inconnue.

Le procédé est le suivant :

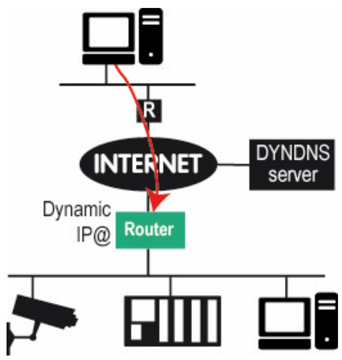
Chaque fois qu'il se connecte à l'Internet, le routeur ETIC inscrit l'adresse IP provisoire qu'il reçoit sur l'Internet auprès du serveur DynDNS ou NoIP à l'emplacement qui lui est réservé (mon_routeur_etictelecom, dans notre exemple).



Chaque fois qu'il souhaite se connecter au produit, le PC ou le routeur distant transmet au serveur DYNDNS une requête visant à obtenir en retour l'adresse IP du routeur ETIC possédant le nom de domaine « mon_routeur_etictelecom ».



Une fois qu'il a acquis l'adresse IP du routeur ETIC, le PC distant peut établir la connexion à travers l'Internet.



11.2 Paramétrage

MISE EN SERVICE

Etape 1 : Ouvrir un compte auprès de DynDNS ou NoIP.org pour réserver un nom de domaine dynamique. C'est le nom que l'on attribue au routeur sur l'Internet (mon_routeur_etictelecom.dyndns.org, par exemple).

Etape 2 : Configurer le routeur

- Sélectionner le menu Configuration > Réseau > Routage > Dyndns.

- Cocher la case « Activer »

Paramètre « Fournisseur de service DNS » :
Choisir DynDNS ou NoIP

Paramètres « Identifiant du compte DNS dynamique » et « Mot de passe » :
Saisir l'identifiant et le mot de passe du compte ouvert chez le fournisseur de service de DNS dynamique.

Paramètres « Hostname» :
Saisir le nom de domaine enregistré chez le fournisseur ; par exemple « mon_routeur_etictelecom ».

12 Interconnexion de routeurs au moyen de VPNs IPSec

12.1 Présentation

Chaque connexion IPSec est un tunnel établi entre deux routeurs.

Ce tunnel VPN permet de connecter deux réseaux de façon sûre et transparente : Lorsque le tunnel est établi entre 2 routeurs, chaque équipement du premier réseau peut échanger des trames IP avec chaque équipement du second.

25 connexions VPN IPSec peuvent être créées.

Le fonctionnement de chaque connexion IPSec est réglé individuellement ce qui permet une grande souplesse d'utilisation.

- **Authentification**

L'authentification réciproque des deux routeurs participants à la connexion peut être réalisée au moyen d'une clé partagée ou de certificats.

Utilisation d'une clé partagée :
La clé partagée est, comme son nom l'indique, un code identique enregistré dans les deux routeurs participant à la connexion. La clé partagée doit être produite par le routeur initiateur auprès du routeur répondeur pour autoriser la connexion.

Utilisation de certificats :
Un certificat X509 est enregistré en usine dans le routeur. Il est produit par l'autorité de certification enregistrée par ETIC TELECOM.

Si nécessaire, il est possible d'enregistrer d'autres types de certificat dans le routeur (voir paragraphe enregistrement de certificats).

Le certificat peut être utilisé pour l'authentification réciproque des routeurs.

Dans ce cas, le routeur initiateur de la connexion présente son certificat au routeur répondeur.
Réciproquement, le routeur répondeur s'authentifie auprès de l'initiateur.

- **Utilisation de IPSec lorsque l'adr. IP source est modifiée le long du trajet (NAT ou adresse IP dynamique)**

Pour garantir l'authenticité de l'initiateur du tunnel, chacun des deux routeurs du tunnel IPSec vérifie si l'adresse IP source n'a pas été modifiée au cours du cheminement dans le réseau.
Pour cette raison, IPSec nécessite un paramétrage particulier lorsque le routeur initiateur ou répondeur est installé de telle sorte que les trames IP franchissent des nœuds (routeurs intermédiaires dans le trajet), qui modifient l'adresse IP source.
C'est ce que font, par exemple, les routeurs de l'opérateur télécom à l'interface entre le réseau cellulaire et l'Internet.

Pour pallier cette difficulté, deux solutions sont possibles :

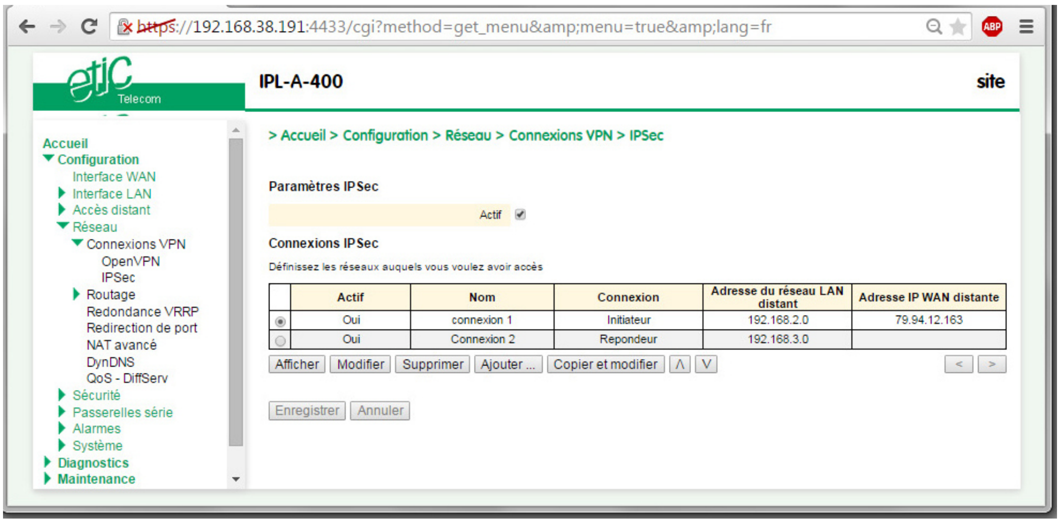
Solution 1 : Utiliser des certificats et pas un clé paratgée.

Solution 2 : Si l'on utilise une clé partagée, il faut attribuer un code d'identité à chaque routeur (IKE ID).
Ce code identifie chaque routeur IPSec auprès de l'autre routeur.
Il faut donc saisir dans chaque routeur le paramètre « IKE ID » du routeur (paramètre « IKE ID local ») et le paramètre « IKE ID » du routeur distant (paramètre IKE ID distant).

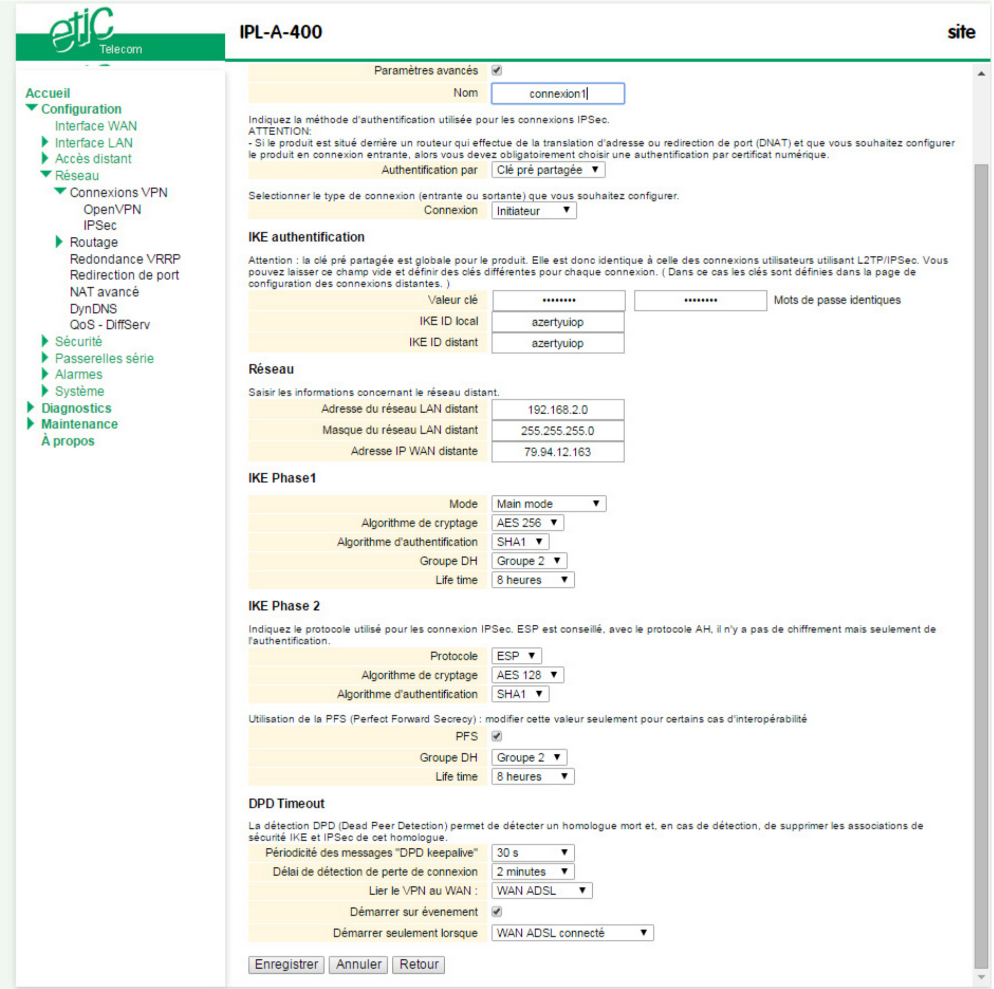
12.2 Paramétrage d'une connexion VPN IPSec

- Sélectionner le menu « **Configuration** », puis « **Réseau** », puis « **Connexions VPN** ».

L'écran des connexions VPN s'affiche.



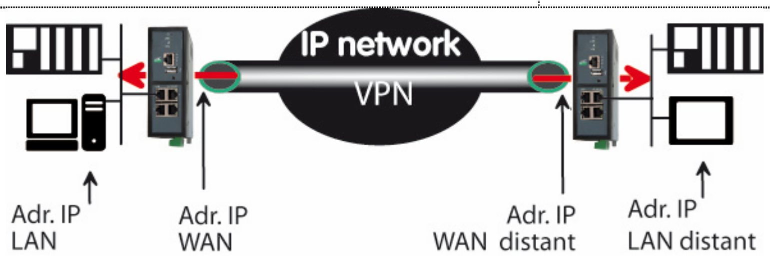
Pour ajouter une connexion VPN IPSec, cliquer « Ajouter ».



L'écran d'une nouvelle connexion VPN IPSec s'affiche.

- Sélectionner la case cocher « Activer » et éventuellement « Paramètres avancés ».
- Attribuer un nom à la connexion.

Les différentes adresses IP auxquelles il est fait référence sont décrites ci-dessous :

Routeur en cours de paramétrage		Routeur distant	
			
192.168.1.0	10.10.10.7	10.10.10.100	192.168.2.0
255.255.255.0			255.255.255.0

Paramètre « Authentification » :
Deux choix sont possibles : Certificat numérique X509 ou Clé partagée.

Paramètre « Connexion » :
Sélectionner la valeur « Initiateur » si la connexion est établie à l'initiative du routeur en cours de paramétrage.

Sélectionner la valeur « Répondeur » si la connexion est établie à l'initiative du routeur distant vers le routeur en cours de paramétrage.

Paragraphe authentification – Cas du choix Certificat numérique

Paramètre « Mon SubjectAlt name » :
Entrez la valeur du champ 'SubjectAltName' du certificat actif du routeur/
Si l'on utilise le certificat enregistré en usine dans le routeur, il s'agit du champ Email.

Paramètre « SubjectAlt name distant» :
Entrez la valeur du champ 'SubjectAltName' du certificat actif du routeur distant.
Pour les certificats ETIC, il s'agit du champ Email.

Paragraphe authentification – Cas du choix clé partagée

Paramètre « Clé » :
Saisir la valeur de la clé partagée nécessaire pour l'authentification du routeur.
la clé, comme son nom l'indique, est identique sur les deux routeurs participant au VPN.

Paramètre « IKE ID local » :
Nom utilisé par le produit pour s'identifier pendant la phase 1.
Il est nécessaire de le remplir si on utilise une clé partagée et dans le cas où un des routeurs IPL est lui-même placé derrière un autre routeur qui translate les adresses source (fonction NAT).

Paramètre « IKE ID distant » :
Nom utilisé par le produit pour identifier son pair pendant la phase 1. Il est nécessaire de le remplir si on utilise une clé partagée et dans le cas où un des routeurs IPl est lui-même placé derrière un autre routeur qui translate les adresses source (fonction NAT).

Paragraphe Réseau

Paramètres « Adresse du réseau LAN distant » et « Netmask distant :
Saisir l'adresse et le netmask du réseau distant (exemple 192.168.2.0 et 255.255.255.0)

Paramètres « Adresse WAN distant » (uniquement si le routeur est initiateur du VPN) :
Saisir l'adresse WAN du routeur distant.

Remarque :
Cette adresse est l'adresse du routeur vers lequel le VPN doit être établie.
Elle ne doit être saisie que si la connexion est de type « initiateur ».

Paragraphe IKE phase 1

IKE est le protocole d'échange de clés. Il se déroule en deux phases.
La phase 1 de IKE est la phase d'établissement d'un canal de sécurité.
La phase 2 est la phase de négociation des paramètres de cryptage des données échangées par les routeurs.
Ce paragraphe permet de choisir les paramètres de la phase 1.

Paramètre « Mode» :
Les modes « Main » et « Agressive » sont proposés.

Le mode « Agressive » est un mode moins sécurisé.

Paramètres «Algorithme de cryptage » :
Sauf difficulté particulière, on sélectionnera le choix « Auto ».
AES offre une meilleure sécurité par que 3DES.

Paramètres «Algorithme d'authentification» :
Sauf difficulté particulière, on sélectionnera le choix « Auto ».
SHA1 offre une meilleure sécurité par que MD5.

Paramètres «Groupe DH» (uniquement si la case « paramètres avancés » a été cochée) :
Groupe utilisé lors de l'échange de clefs Diffie-Hellman (DH). Le DH est l'étape 1 de la phase 1 et permet aux pairs de se mettre d'accord sur un secret partagé. Le DH a besoin qu'un groupe (au sens structure algébrique) soit défini et identique sur les pairs pour fonctionner. Plus le groupe est grand, plus la sécurité est élevée, au détriment du temps d'établissement du VPN. Recommandé : groupe 2.

La même valeur doit être choisie dans les 2 routeurs participant au VPN.

Paramètres «Life-time» (uniquement si la case « paramètres avancés » a été cochée) a été cochée) :
Saisir la durée de vie de la clé.

Paragraphe IKE phase 2
La phase 2 de IKE est la phase de négociation des paramètres de cryptage des données échangées par les routeurs.

Paramètres «Protocole» :
Préférer ESP à AH.
ESP assure confidentialité, intégrité et authentification des paquets échangés par les routeurs.
AH assure intégrité et authentification mais pas la confidentialité (ou cryptage).

Paramètres «Algorithme de cryptage » :
Sauf difficulté particulière, on sélectionnera le choix « Auto ».
AES offre une meilleure sécurité par que 3DES.

Paramètres «Algorithme d'authentification» :
Sauf difficulté particulière, on sélectionnera le choix « Auto ».
SHA1 offre une meilleure sécurité par que MD5.

Case à cocher «PFS» :
PFS (Perfect forward Secrecy) garantit qu'un attaquant ayant enregistré des échanges chiffrés à un instant donné et parvenant à obtenir les secrets cryptographiques à une date ultérieure ne puisse pas pour autant déchiffrer les enregistrements.

Le renouvellement périodique de la clé renforce la sécurité.

Paramètres «Groupe DH» (uniquement si la case « PFS a été cochée) :
Groupe utilisé lors de l'échange de clefs Diffie-Hellman (DH). Le DH est l'étape 2 de la phase 1 et permet aux pairs de se mettre d'accord sur un secret partagé. Le DH a besoin qu'un groupe (au sens structure algébrique) soit défini et identique sur les pairs pour fonctionner. Plus le groupe est grand, plus la sécurité est élevée, au détriment du temps d'établissement du VPN. Recommandé : groupe 2.

La même valeur doit être choisie dans les 2 routeurs participant au VPN.

Paramètres «Life-time» (uniquement si la case « PFS a été cochée) :
Saisir la durée de vie de la clé de la phase 2.

Paragraphe DPD time-out
Paramètre « Période des messages DPD Keepalives » :
Le VPN est entretenu périodiquement par chaque routeur ; pour ce faire, et en l'absence de données à émettre, chaque routeur transmet une trame de maintien du VPN.
Ce paramètre fixe la période d'envoi de la trame de maintien du VPN par le routeur.

Paramètre « Délai de détection de perte de connexion » :
Ce paramètre fixe le délai maximum d'attente d'un message Keep-alive.
Une fois ce délai échu, et en l'absence de réception du message Keep alive, le routeur coupe le VPN.

13 Connexion VPN de type OpenVPN

13.1 Présentation

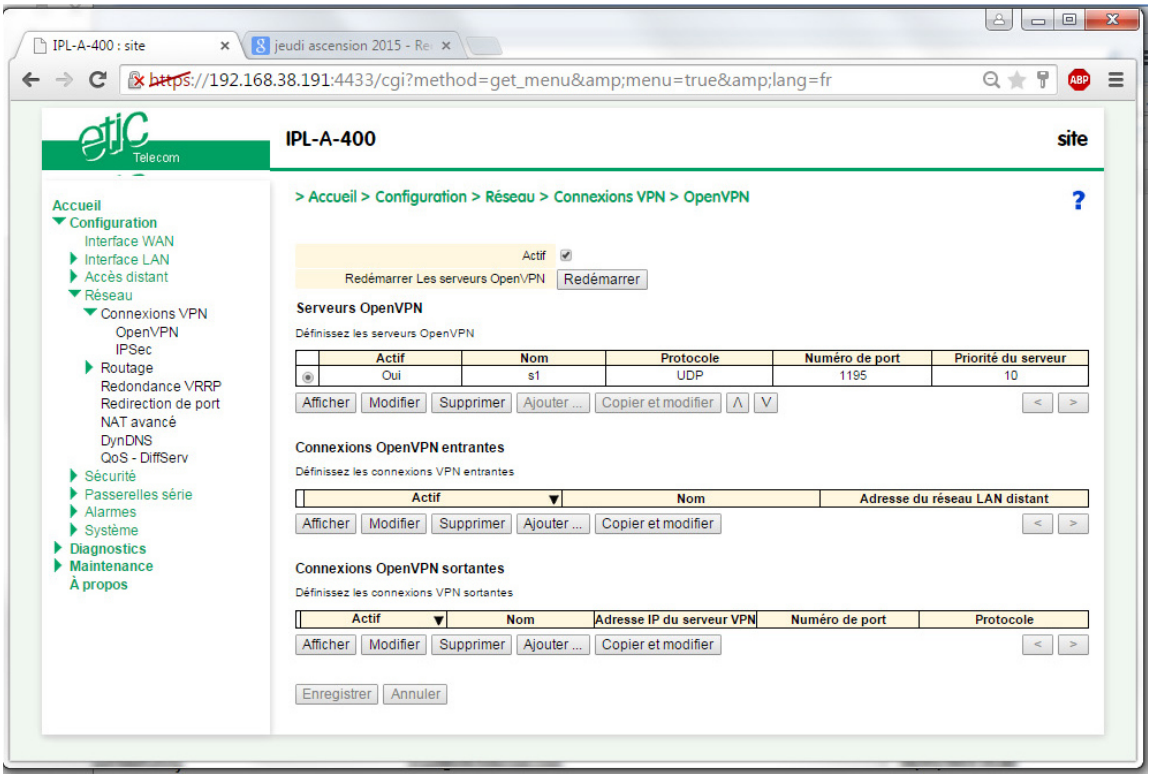
Chaque connexion VPN de type OpenVPN est un tunnel établi entre deux routeurs.

Ce tunnel VPN permet de connecter deux réseaux de façon sûre et transparente : Lorsque le tunnel est établi entre 2 routeurs, chaque équipement du premier réseau peut échanger des trames IP avec chaque équipement du second.

25 connexions VPN peuvent être créées.

- Pour configurer les connexions OpenVPN, sélectionner le menu Configuration > Réseau > OpenVPN.

L'écran des connexions VPN s'affiche.



13.1.1 Etapes de la configuration

Le paramétrage des connexions VPN s’effectue en 2 étapes :

Etape 1 : Configuration du protocole VPN lui-même

Etape 2 : Configuration des connexions VPNs.

Le routeur qui initie la connexion VPN établit une connexion sortante vers le routeur serveur VPN qui accepte une connexion entrante.



Le routeur initie la connexion VPN
Pour ce routeur, la connexion est sortante
Ce routeur est le client VPN

Le routeur accepte la connexion VPN
Pour ce routeur, la connexion est entrante
Ce routeur est le serveur VPN

13.1.2 Authentification

L’extrait du certificat de chaque routeur client VPN doit être enregistré dans le routeur serveur VPN.

Lorsqu’il initie la connexion VPN, le routeur client VPN, s’authentifie auprès du serveur en présentant son propre certificat.

13.1.3 Contraintes de paramétrage

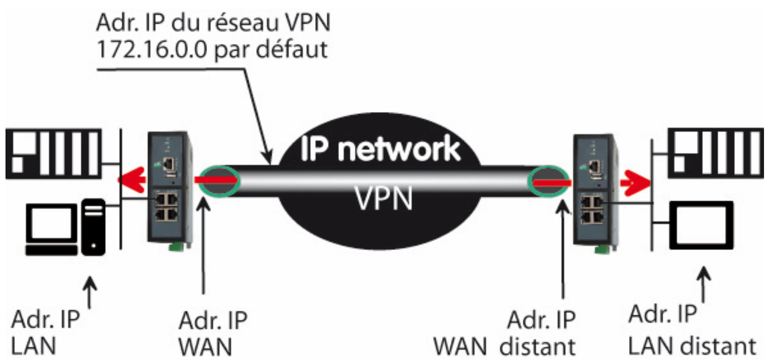
Les paramètres de N° de port et de protocole de transport (UDP ou TCP) doivent être identiques dans le serveur VPN et dans tous les clients.

Les valeurs des paramètres de chiffrement (Blowfish, AES 256, AES192, AES128, 3DES) et d’authentification (MD5, SHA1) doivent être identiques dans le serveur VPN et dans tous les clients.

Le réseau « LAN » et le réseau « LAN distant » doivent être différents.

Par exemple :

Réseau LAN :	192.168.1.0	netmask 255.255.255.0
Réseau LAN distant :	192.168.2.0	netmask 255.255.255.0



Routeur en cours de configuration

Serveur VPN

13.2 Paramétrage du serveur OpenVPN

- Dans le tableau « Serveur VPN », sélectionner le bouton « Ajouter ».

(*) Paramètres «Numéro de port» et « protocole» :
On choisira de préférence le protocole UDP plutôt que TCP pour une meilleure efficacité.

Attention :
Le numéro de port utilisé pour l'interconnexion de routeurs par VPN doit être différent du N° de port utilisé pour les connexions d'utilisateurs distants.

(*) Paramètres « Adresse réseau VPN » et masque réseau VPN :
Le tunnel VPN une fois établi est équivalent à une liaison par câble Ethernet. Chaque extrémité du tunnel doit avoir une adresse IP. Il s'agit d'une adresse IP appartenant à un réseau privé et nécessaire pour le fonctionnement du tunnel, mais non visible pour les applications. Cette adresse IP ne doit pas être confondue avec l'adresse IP du routeur sur le réseau IP. Cette valeur est utilisée seulement lors de la configuration d'un nœud entrant.

Paramètre « délai de détection de perte de connexion » :
En l'absence de données à émettre, le VPN est entretenu périodiquement par le routeur client au moyen d'un paquet de contrôle transmis vers le serveur.
A l'issue de cette période et en l'absence de réception de ce paquet, le VPN est coupé.
Ce paramètre fixe la période d'envoi du paquet de contrôle.

Remarque :

Ce paramètre doit être fixé avec attention ; en effet, en cas d'interruption du VPN, il détermine le délai qu'attend le routeur avant de le relancer ; pendant toute cette durée, la communication entre les routeurs sera donc impossible.

Prenons un exemple :
Si on fixe ce paramètre à 15 minutes, et en cas d'interruption de la connexion pour une raison quelconque, la communication sera impossible pendant 15 minutes maximum (en moyenne, la moitié, soit 7 mn 30).
Si on fixe la valeur à 1 mn, le temps d'interruption ne sera que de 1 mn au maximum., mais l'envoi périodique du paquet de contrôle peut engendrer un trafic coûteux ou gênant sur un réseau 4G ou 3G.

Paramètre « Délai de retransmission » :
C'est le délai au bout duquel le routeur ré-émet le paquet de contrôle en l'absence d'acquittement.

(*) Paramètres « Chiffrement » & « Authentification» :
Les algorithmes de cryptage et de hachage proposés sont tous d'un haut niveau de sécurité (par exemple l'ancien algorithme DES n'est pas proposé). Toutefois, AES offre une meilleure sécurité par rapport à 3DES, de même que SHA-1 par rapport MD5.

Paramètre « Priorité du serveur » :
C'est le délai au bout duquel le routeur ré-émet le paquet de contrôle en l'absence d'acquittement.

Paramètre « Pousse la route locale aux clients VPN» :
Laisser cette case cochée.
Dans ce cas, le serveur indique à tous les clients VPN qu'il faut passer par le VPN pour atteindre le réseau LAN du serveur.

Paramètre «Pousse les routes statiques aux clients VPN» :
Dans ce cas, le serveur indique à tous les clients VPN qu'il faut passer par le VPN pour atteindre les réseaux accessibles par les routes statiques du serveur VPN.

Paramètre « Pousse les routes aux clients VPN» :
Cette fonction est utile pour permettre à un équipement raccordé à un client VPN d'échanger des données avec un autre équipement raccordé à un client VPN (client to client).

Le serveur VPN a connaissance de la route qui mène à chaque réseau raccordé à chaque routeur client VPN.

- Si cette case n'est pas sélectionnée, un équipement raccordé à un routeur client VPN peut échanger des trames IP avec un équipement raccordé au serveur VPN.
  Mais il ne peut pas échanger des trames IP avec un équipement raccordé à un autre routeur client VPN.

Pour que des équipements raccordés à deux routeurs clients VPN différents puissent échanger des trames, il faut enregistrer une route statique dans chaque routeur client VPN, ou bien cocher la case.

- Si cette case est sélectionnée, le serveur diffuse ces routes vers tous les clients.
  Ainsi, tout équipement raccordé à un routeur client VPN peut échanger des trames IP avec tout autre équipement raccordé à un autre routeur sans qu'il soit nécessaire de programmer des routes.

Paramètre « 1ere route spécifique à pousser / adresse IP et netmask» :
Envoie aux clients les chemins : "la valeur du paramètre" via "le VPN"

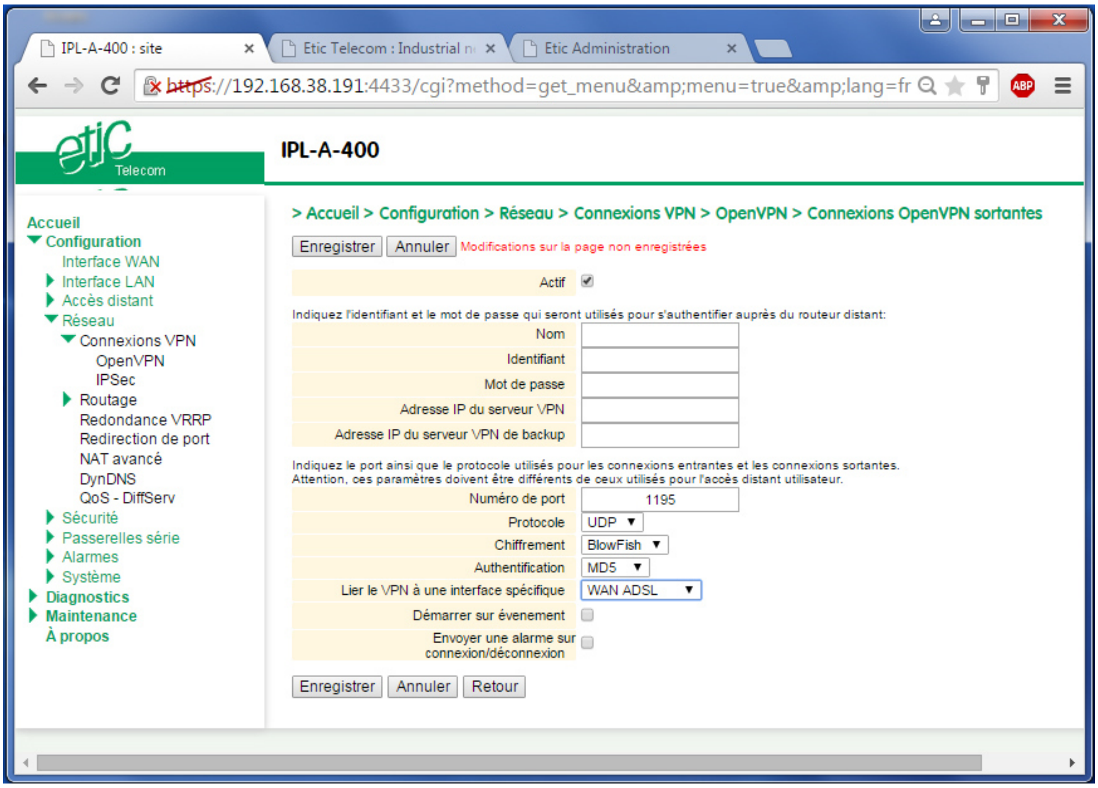
Paramètre « 2eme route spécifique à pousser / adresse IP et netmask» :
Envoie aux clients les chemins : "la valeur du paramètre" via "le VPN"

13.3 Configurer une connexion OpenVPN sortante

La valeur des paramètres précédés d'une « * » doit être identique dans tous les routeurs du réseau y-compris le serveur.

Une connexion sortante est une connexion VPN établie à l'initiative du routeur.

- Pour créer une connexion sortante, cliquer le bouton « **Ajouter**» placé sous le tableau des connexions sortantes.



- Sélectionner la case cocher « Actif » et attribuer un nom à la connexion.

Paramètres « Identifiant et mot de passe » :
Saisir l'identifiant et le mot de passe qui seront utilisés par le routeur pour s'authentifier auprès du serveur VPN en complément du certificat.

Remarque : Cet identifiant et ce mot de passe devront donc être enregistrés dans la connexion entrante du serveur VPN.

Paramètre « Adresse IP du serveur VPN » :
C'est l'adresse vers laquelle le tunnel VPN doit être établi.

Cette adresse peut être soit l'adresse IP fixe Internet du routeur distant, soit son nom de domaine sur DynDns.org ou NoIP, soit son nom de domaine.

Paramètre « Adresse IP du serveur VPN de backup» :
Ce paramètre permet de désigner un serveur VPN de secours.
Si le serveur principal n'est pas accessible le routeur IPL établit le VPN avec le serveur de secours.

En l'absence de serveur de secours, laisser ce champ vide.

(*) Paramètres «Numéro de port» et « protocole» :
On choisira de préférence le protocole UDP plutôt que TCP pour une meilleure efficacité.

(*) Paramètres « Chiffrement » & « Authentification» :
Les algorithmes de cryptage et de hachage proposés sont tous d'un haut niveau de sécurité (par exemple l'ancien algorithme DES n'est pas proposé).
Toutefois, AES offre une meilleure sécurité par rapport à 3DES, de même que SHA-1 par rapport MD5.

Paramètres « lier le VPN à une interface spécifique» :

Lier le VPN à l'interface cellulaire
Une connexion VPN sortante de type OpenVPN est habituellement établie via l'interface WAN principale du routeur IPL; par exemple l'interface cellulaire dans le cas du routeur IPL-C.

- Pour forcer l'établissement du VPN vers l'interface cellulaire, assigner au paramètre la valeur « WAN cellulaire ».

Lier le VPN à l'interface Ethernet WAN ou à l'interface WiFi
Le VPN peut aussi être forcé vers l'interface Ethernet N°1 lorsque l'interface cellulaire a été désactivée et remplacée par l'interface Ethernet N°1 (Interface Ethernet WAN).

- Pour forcer l'établissement du VPN vers l'interface Ethernet N°1 lorsqu'elle a été activée comme interface WAN à la place de l'interface cellulaire, assigner au paramètre la valeur « WAN Ethernet ».

- Pour forcer l'établissement du VPN vers l'interface WiFi lorsqu'elle a été activée comme interface WAN à la place de l'interface cellulaire, assigner au paramètre la valeur « WAN WiFi».

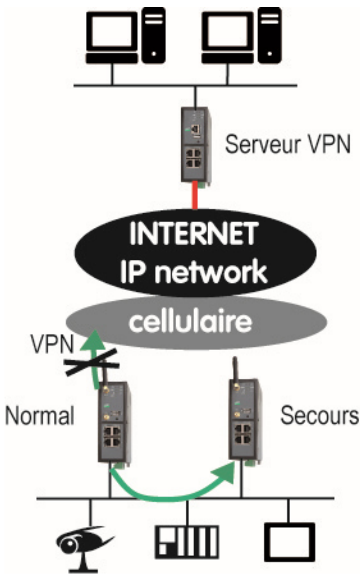
Associer le VPN à l'interface disponible pour créer une solution redondante

Enfin, on peut souhaiter créer une solution redondante permettant de transmettre par une autre liaison et au moyen d'un autre routeur lorsque la liaison cellulaire est défaillante.

Pour permettre au VPN de s'établir vers l'interface LAN à la place de l'interface cellulaire , assigner au paramètre la valeur « Tous ».

L'adresse LAN du routeur « Secours » doit être saisie comme passerelle par défaut dans le routeur « Normal » (menu Interface LAN > Ethernet et IP).

L'adresse LAN du routeur « Normal » doit être saisie comme passerelle par défaut dans le routeur « Secours » (menu Interface LAN > Ethernet et IP).



Remarque : Cette solution protège contre la défaillance de la connexion cellulaire ; pour s'affranchir en plus de la défaillance du routeur lui-même, il faut activer le protocole VRRP.

Valeur	Observation
WAN cellulaire	Le VPN ne peut s'établir que par l'interface cellulaire
WAN Ethernet	Le VPN ne peut s'établir que par l'interface Ethernet N°1 lorsqu'il est déclaré comme WAN en remplacement de l'interface cellulaire
WAN WiFi	Le VPN ne peut s'établir que par l'interface WiFi lorsqu'il est déclaré comme WAN en remplacement de l'interface cellulaire
Tous	Le VPN s'établit par l'interface WAN actif (Interface cellulaire habituellement) et, si elle devient indisponible, par l'interface LAN. Le VPN s'établit à nouveau par l'interface ADSL quand elle redevient disponible. De cette façon, on créé une solution redondante

Case à cocher « Démarrer sur événement » :

Le VPN est habituellement établi par le routeur dès la mise sous tension.
Cependant, il peut être intéressant de pouvoir commander l'établissement du VPN.

Il est possible de déclencher l'établissement du VPN sur l'un des événements suivants :

- WAN cellulaire connecté
- WAN cellulaire déconnecté
- WAN Ethernet connecté
- WAN Ethernet déconnecté
- Entrée digitale fermée
- Entrée digitale ouverte

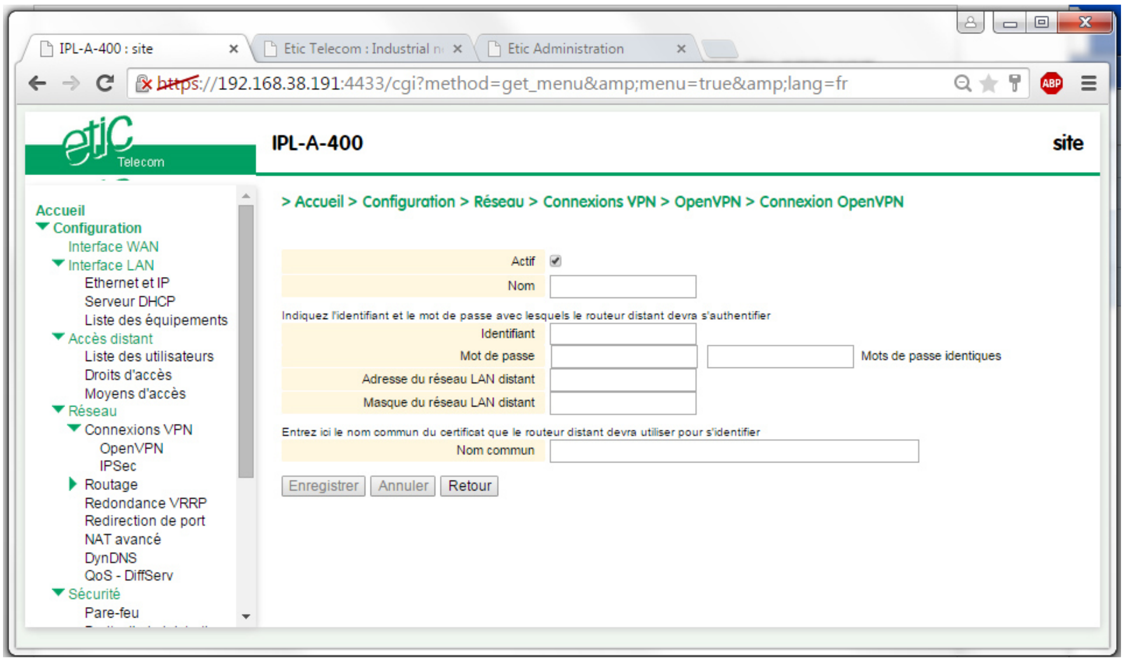
Case à cocher « Envoyer une alarme sur connexion / déconnexion » :

Ce VPN génère un évènement qui peut être traité dans la page web "alarmes, sms/email" lorsque on choisit comme source d'alerte connexion / déconnexion VPN.

13.4 Configurer une connexion OpenVPN entrante

Une connexion sortante est une connexion VPN établie à l'initiative du routeur.

- Pour créer une connexion entrante, cliquer le bouton « **Ajouter**» placé sous le tableau des connexions entrantes.



- Sélectionner la case cocher « Actif » et attribuer un nom à la connexion.

Paramètres « Identifiant et mot de passe » :
Saisir l'identifiant et le mot de passe qui seront présentés par le routeur distant pour s'authentifier.

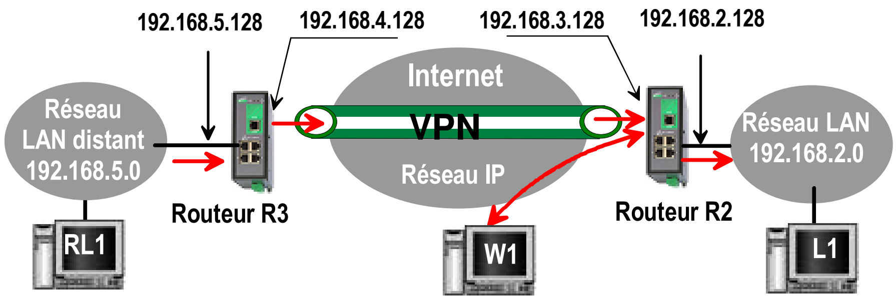
Paramètres « Adresse IP du LAN distant » & « Masque du réseau LAN distant»:
Saisir l'adresse du réseau LAN du routeur distant.

Paramètre « Nom commun» :
Entrez la valeur du champ 'SubjectAltName' du certificat actif du routeur distant.
Pour les certificats ETIC, il s'agit du champ Email.

14 Routage

14.1 Fonctions de base

Le routeur R2 (voir schéma ci-dessous) est prêt à effectuer sa fonction de routeur entre le réseau LAN et l'Internet dès qu'on lui a attribué une adresse IP sur l'interface LAN (ici 192.168.2.128) et une autre sur l'Internet et que l'on a configuré la connexion Internet.



Pour que le routage s'effectue, Il faut cependant enregistrer dans chaque machine du réseau LAN l'adresse LAN du routeur IPL-C en tant « routeur par défaut ».

Le routeur R2 peut alors router des trames IP entre le réseau «LAN» et le réseau LAN distant au travers du VPN s'il a été défini; par exemple entre la machine RL1 et la machine L1 du schéma ci-dessus. En effet, par défaut, le firewall autorise le transfert entre les deux réseaux si un VPN relie les routeurs.

Par contre, par défaut, les paquets IP émis par la machine W1 depuis l'internet sont bloqués par le firewall.

14.2 Route statique

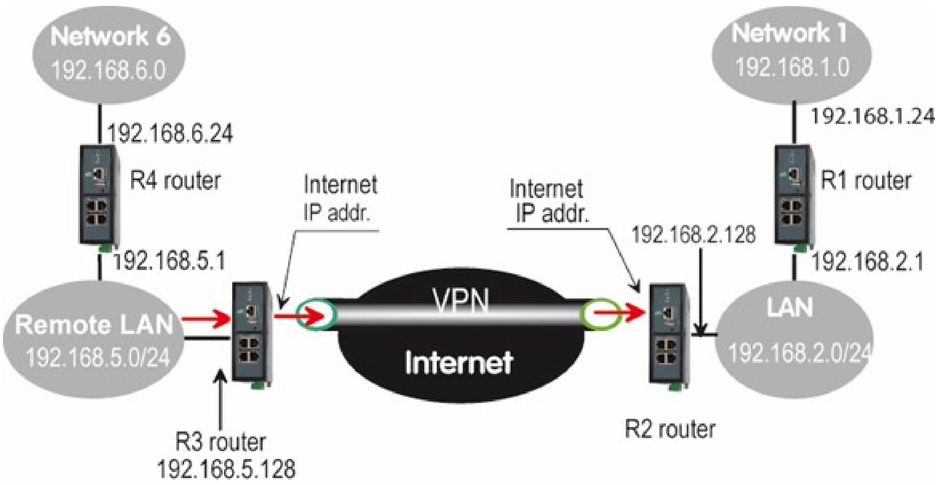
Après avoir configuré ses adresses LAN et WAN et défini la connexion VPN, le routeur R2 (voir schéma ci-dessus) peut router les trames entre le réseau LAN et le WAN et inversement, ainsi qu'entre le LAN et le réseau Remote LAN et inversement au travers du VPN.

Mais il ne peut pas router des trames entre le LAN et un réseau connecté au réseau LAN distant (réseau 6 du schéma ci-dessous).

La raison de cette difficulté est que le réseau 6 n'est pas connu du routeur R2.

La déclaration de routes statiques permet de résoudre ce problème.

Une route statique associe l'adresse d'un routeur voisin à une adresse IP de réseau de destination (adr. Réseau = adr. de base + netmask).



On décrit ci-dessous les routes statiques qui doivent être enregistrées dans le routeur R2 pour que tous les équipements de chacun des réseaux puissent échanger des paquets IP.

Route statique à enregistrer dans le routeur R2						
Active	Nom de la route	Destination	Masque de réseau	Passerelle	Interface	Distance
Oui	Vers Réseau 6	192.168.6.0	255.255.255.0	192.168.5.1		
Oui	Vers Réseau 1	192.168.1.0	255.255.255.0	192.168.2.1		
Oui	Vers Réseau WAN distant	192.168.4.0	255.255.255.0	192.168.5.128		

De la même façon, il faut enregistrer des routes dans les routeurs R1, R3 et R4.

Remarque :
Il n'est pas nécessaire d'enregistrer dans R2 une route vers le réseau WAN ni vers le réseau LAN distant; en effet, R2 les connaît puisque l'adresse et le netmask du réseau WAN ainsi que l'adresse du réseau LAN distant ont été déclarés au cours de la configuration.

Pour programmer une route statique,

- sélectionner le menu « Configuration », puis « Routage » puis « Route statique » puis cliquer « Ajouter une route ».

Paramètre « Nom de la route » :
Entrer un mnémonique pour désigner la route.

Paramètres «Adresse IP de destination » & « netmask » :
Entrer l'adresse IP du réseau de destination et le netmask de ce réseau.

Paramètre «Passerelle » :
Saisir l'adresse IP de la passerelle (routeur) permettant l'accès à ce réseau.

Paramètre «Interface » :
Une route peut être établie en désignant une passerelle (voir ci-dessus) ou bien une interface.
Par exemple : On peut désigner une route passant par l'interface PPoE du port Ethernet N°1.

Si une route est établie en désignant l'adresse d'une passerelle, laisser ce champ vide.

Paramètre «Priorité » :
Le paramètre de priorité s'applique à chaque route statique de la même manière qu'aux liaisons VPNs.

Lorsque deux routes mènent au même réseau de destination, le routeur sélectionne la route la plus prioritaire.

Le degré de priorité est décroissant : Une route de de priorité 10 est plus prioritaire qu'une route de priorité 20.

Remarque :
Ce champ ne doit pas être laissé vide; en l'absence de nécessité de désigner une priorité, saisir la même valeur, 10 par exemple, pour chacune des routes.

14.3 Protocole RIP

RIP (**Routing Information Protocol**) est un protocole de routage IP qui permet à chaque routeur d'un réseau de connaître la route menant à un sous réseau quelconque de ce réseau.

Le principe utilisé est le suivant :

Diffusion des tables de routage
Chaque routeur transmet aux routeurs voisins et aux écouteurs RIP voisins, la table qui associe à chaque destination du réseau l'adresse du routeur voisin menant à cette destination ainsi que la métrie de la route pour y parvenir.

Mise à jour des tables de routage
Chaque routeur met à jour sa propre table au moyen des informations reçues des autres.

Le protocole RIP permet d'éviter de déclarer les routes statiques dans chacun des routeurs.

Prenons l'exemple du réseau du paragraphe précédent ; au lieu de déclarer les routes statiques dans les routeurs R1, R2, R3 et R4, il est possible d'activer le protocole RIP dans chacun des routeurs.

Pour activer le protocole RIP,

- sélectionner le menu Configuration > Routage > RIP.

Cocher les cases «Activer RIP sur l'interface LAN » et la case Activer RIP sur l'interface WAN ».

15 Substitution d'adresses (NAT, Redirection de port, NAT avancé)

Le routeur IPL offre différentes fonction de substitution d'adresses IP.

Ces fonctions consistent à remplacer l'adresse IP et le port source ou destination de certaines trames IP traitées par le routeur.

Les possibilités offertes sont les suivantes :

15.1 Translation d'adresse (NAT)

Cette fonction s'applique aux trames IP issues d'un équipement du réseau LAN et destinées au réseau WAN.

Elle consiste à remplacer l'adresse IP source (celle de l'équipement du LAN) par l'adresse IP WAN du routeur et à effectuer l'opération inverse pour les trames de réponse.

Cette fonction est utile lorsque les équipements du LAN doivent échanger des trames avec l'Internet.

Pour activer la fonction NAT,

- sélectionner le menu Configuration > Interface WAN
- Cocher la case « Activer la translation d'adresse NAT ».

15.2 Redirection par port

15.2.1 Principe

La redirection de port consiste à transférer vers une machine définie du réseau LAN, un trafic adressé au routeur IPL sur son interface WAN.

Elle s'applique aux trames adressées au routeur IPL sur l'interface WAN.

Le critère de « redirection » est le N° du port utilisé ; le mécanisme consiste à utiliser le N° de port de destination comme un complément d'adresse IP :
Une trame IP adressée sur l'interface WAN au routeur IPL sur le port déterminé P1 (ou un ensemble de ports) peut être redirigée vers un équipement déterminé du réseau LAN.

Le mécanisme de redirection de port décrit ci-dessus permet de résoudre le cas où un équipement appartenant au réseau WAN veut échanger des trames IP avec une ou des équipements du réseau LAN alors que les adresses du réseau LAN ne peuvent être transportées dans le réseau WAN.

La vraie solution à ce problème est d'établir un VPN ; mais lorsque ce n'est pas possible la redirection de port apporte la solution.

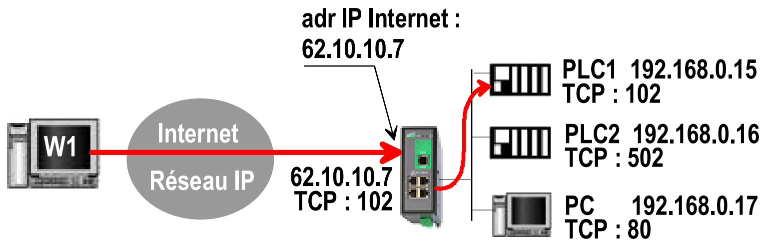
Exemple :
Considérons un réseau 1 et un réseau 2 connectés par un routeur IPL selon le schéma ci-dessous.

Supposons

1/ que le PC « W1 » du réseau WAN ait à échanger des trames avec l'équipement PLC1 du réseau LAN.

2/ que les adresses du réseau LAN ne puissent pas circuler sur le réseau WAN, quelle que soit la raison.

La solution la plus performante serait d'établir un VPN qui assurerait à la fois la transparence et la sécurité ; si ce n'est pas possible, on peut procéder comme suit :



Lorsque le PC « W1 » doit adresser une trame à l'équipement « PLC1 » du réseau LAN, il l'adresse à l'adresse IP WAN du routeur IPL-C (62.10.10.7 dans notre exemple) et sur le port 102 (par exemple).
Le routeur IPL-C analyse la trame, modifie l'adresse IP de destination et éventuellement le N° de port, puis route la trame vers le réseau LAN.

Port (destination)	Redirection	
Service	Device	Service
102	192.168.0.15	102
502	192.168.0.16	502
80	192.168.0.17	80

Note :
Les trames IP « redirigées » sont transférées directement à l'équipement choisi sans passer par le filtre principal du firewall.

15.2.2 Configuration

Pour programmer une règle de redirection de port,

- Sélectionner le menu Configuration > Réseau, Routage, et Redirection de port.
- Saisir les caractéristiques des trames qui doivent être redirigées : N° de port (de destination), protocole de transport (TCP, UDP…), adresse IP source (optionnelle).
- Saisir les caractéristiques des trames modifiées : Adresse IP et N° de port de destination, et protocole de transport (TCP, UDP…).

15.3 Substitution généralisée d'adresses IP (NAT avancé)

15.3.1 Principe

La fonction de substitution d'adresses IP consiste à modifier les adresses de source et / ou de destination ainsi que le N° de port des trames IP qui transitent par le routeur.

Elle s'applique à toute trame IP reçue par le routeur aussi bien sur son interface LAN que sur son interface WAN hormis aux trames véhiculées dans une connexion d'utilisateur distant PPTP ou TLS.

Elle s'applique aux trames dont la destination est le routeur IPL-C lui-même aussi bien qu'aux trames dont la destination est un équipement du réseau relié directement ou non à l'interface WAN ou à l'interface LAN.

On distingue

la fonction DNAT qui consiste à remplacer l'adresse IP et le port de destination,

la fonction SNAT qui consiste à remplacer l'adresse IP source.

Puisque cette fonction consiste à modifier les adresses de source et / ou de destination des trames IP qui transitent par le routeur, il est important de préciser si le firewall traite des trames IP dont les adresses ont été déjà substituées ou non.

L'ordre dans lequel s'effectue la substitution modifie en effet la manière de configurer les règles du filtre principal du firewall. Les traitements de substitution s'effectuent comme suit :

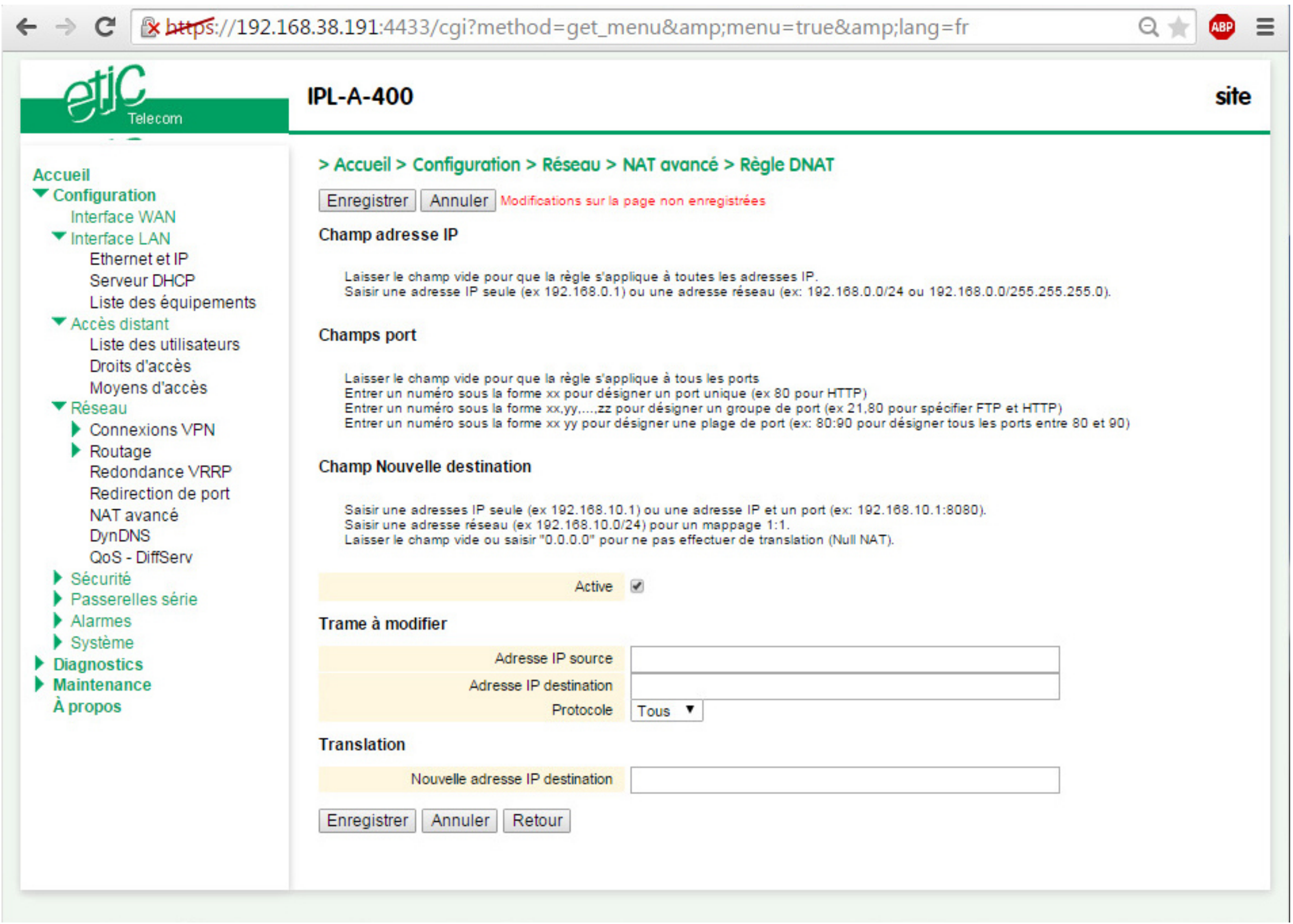
Direction	
WAN vers le LAN	**WAN — DNAT — Routeur — FIREWALL — SNAT → LAN**
LAN vers le WAN	**WAN ← SNAT — FIREWALL — Routeur — DNAT — LAN**

La fonction de substitution décrite ci-dessus (on dit aussi translation) est utile dans des cas très particuliers : Pour router des trames par un chemin de secours, par exemple, ou encore pour adapter un réseau ancien à un nouveau plan d'adresses IP (Mapping).

15.3.2 Configuration

POUR METTRE EN ŒUVRE LA FONCTION NAT AVANCEE,

- sélectionner le menu Configuration > Réseau > Routage > NAT avancé.



Pour créer une règle de substitution d'adresse de destination (DNAT),

- cliquer sur le bouton « Ajouter une règle ». La fenêtre de création s'affiche :

- Sélectionner Oui pour rendre la règle active.

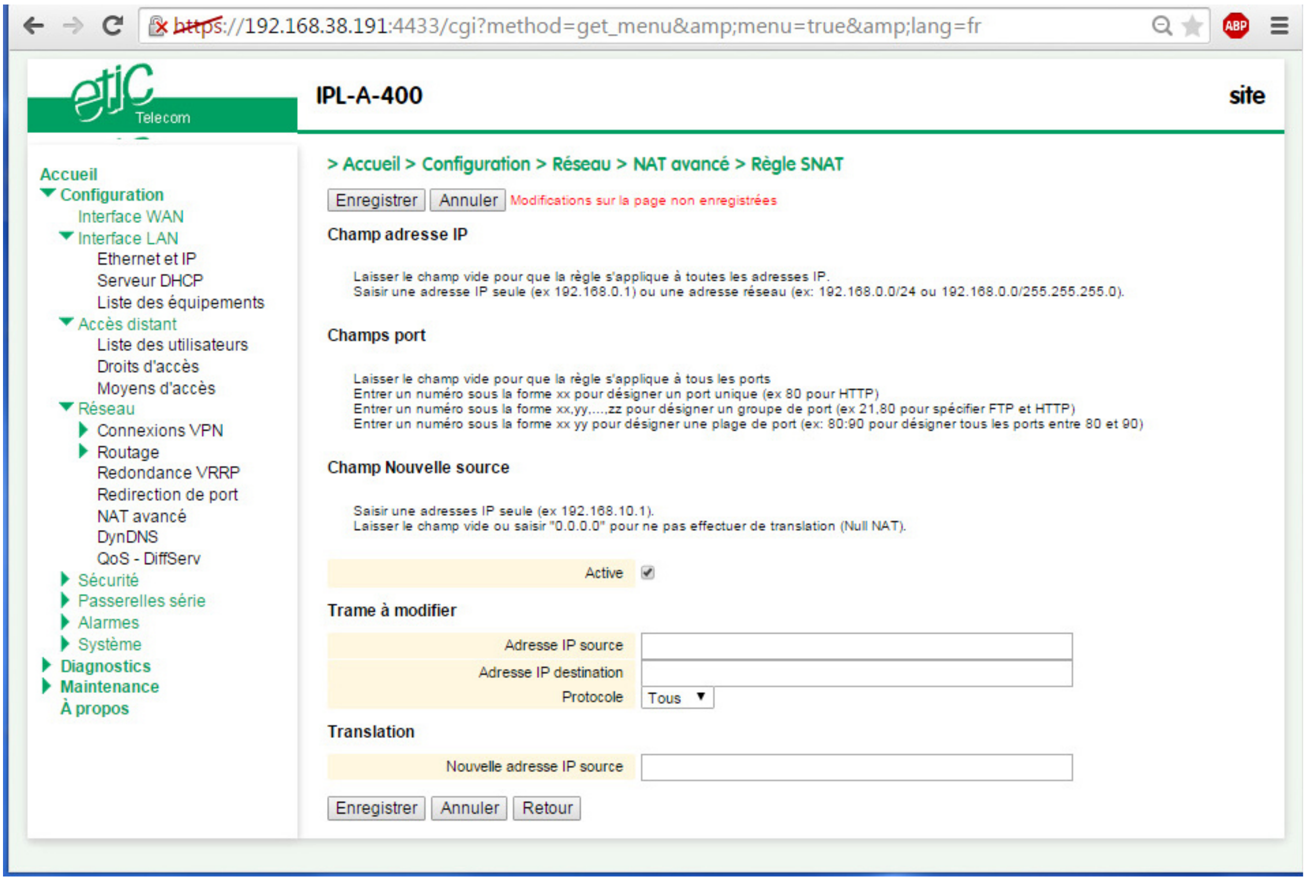
- Saisir les critères de substitution :

Adr. IP source
Adr. IP destination
Protocole (TCP, UDP, …)
Port source
Port destination

- Saisir la nouvelle destination des trames répondant aux critères décrits ci-dessus : Adr. IP et port de destination.

Pour créer une règle de substitution d'adresse source (SNAT),

- cliquer sur le bouton « Ajouter». La fenêtre de création d'une règle SNAT s'affiche :



- Sélectionner « Oui » pour rendre la règle active.

- Saisir les critères de substitution :

Adr. IP source
Adr. IP destination
Protocole (TCP, UDP, …)
Port source
Port destination

- Saisir la nouvelle destination des trames répondant aux critères décrits ci-dessus : Adr. IP source.

16 Redondance VRRP

16.1 Principe

VRRP est un protocole qui permet à deux ou plusieurs routeurs sur un même réseau IP d'agir en redondance les uns des autres afin d'augmenter la disponibilité de la fonction de routeur.

Le mécanisme est le suivant : Les routeurs placés en redondance les uns des autres possèdent chacun une adresse IP, comme tout équipement d'un réseau IP ; mais ils possèdent aussi une adresse IP commune appelée adresse IP virtuelle.

Cette adresse IP virtuelle et partagée est l'adresse IP qui doit être enregistrée dans les différents équipements du réseau comme l'adresse du routeur par défaut.

De plus un indice de priorité (compris entre 1 et 255) est attribué à chacun des routeurs du groupe.

Les routeurs du groupe élisent le routeur maître ; c'est celui qui a l'indice de priorité le plus élevé ; par la suite, il annoncera 255 comme indice de priorité, tandis que les autres routeurs que l'on désignera comme routeur de secours resteront silencieux.

Le routeur maître prend en charge la fonction de routeur ; il répond aux requêtes ARP émises par les équipements du réseau.

De plus, il diffuse régulièrement un message de présence au moyen de l'adresse multicast 224.0.0.18 avec un numéro de protocole IP 112.

A défaut de recevoir le message, un nouveau routeur maître est élu.

Le routeur IPL gère ce protocole aussi bien sur l'interface LAN.

16.2 Configuration

Paramètres « Activer VRRP sur l'interface LAN» :

Cocher cette case pour activer VRRP sur l'interface LAN.

Paramètres « Identité VRRP (1-255)» :

Affecter un code d'identité au groupe de routeurs entre 1 et 255.

Tous les routeurs du même groupe doivent posséder le même code.
Deux groupes différents ne peuvent posséder le même code.

Paramètres « Adresse IP virtuelle » :

Enregistrer l'adresse IP virtuelle commune à tous les routeurs du groupe

Tous les routeurs agissant en redondance doivent posséder la même adresse IP virtuelle.

Paramètres « Indice de priorité VRRP (1-255)» :

Affecter un indice de priorité au routeur entre 1 et 255.

L'indice le plus élevé désigne le routeur le plus prioritaire.

Paramètres «adresse MAC virtuelle» :

On peut associer une adresse MAC virtuelle à l'adresse IP virtuelle.

De cette manière, lorsqu'un équipement du réseau transmet une requête ARP, le maître du groupe VRRP répond toujours avec la même adresse MAC.

L'adresse MAC utilisée est une adresse prévue à cet effet : 00-00-5E-00-01-XX, le dernier octet étant le numéro du groupe VRRP codé en hexadécimal.

17 Service d'accès sécurisé d'utilisateurs distants (RAS)

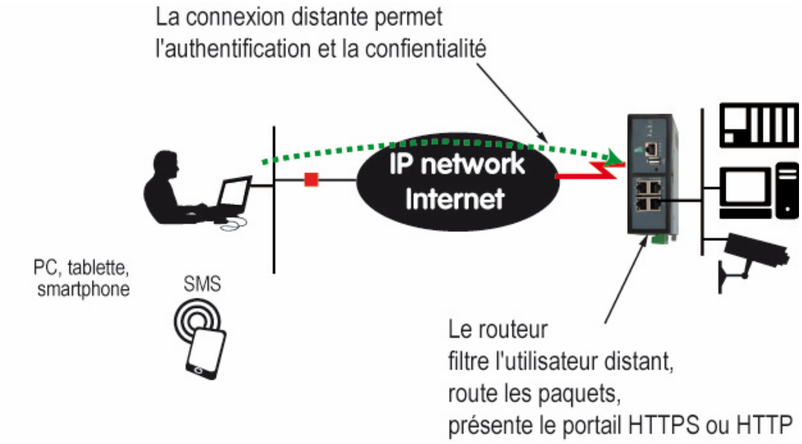
Le routeur IPL-C permet aux utilisateurs distants de se connecter à une machine, simplement et avec un niveau de sécurité élevé en établissant une connexion distante pour réaliser les opérations de télé-exploitation ou télémaintenance, par exemple.

Une fois identifié, l'utilisateur distant peut accéder aux différents équipements du réseau comme s'il était sur place.

Les données peuvent être chiffrées pour la confidentialité.

Le routeur IPL-C permet d'attribuer à chaque utilisateur des droits d'accès individualisés : Un utilisateur peut accéder à tel «équipement ou groupe d'équipements tandis qu'un autre peut accéder à d'autres équipements.

La fonction « portail » est destinée à la consultation des pages web d'automates ou de HMI ; elle permet à l'utilisateur d'un smartphone (ou d'une tablette, ou d'un PC) de consulter les serveurs web embarqués en procurant un niveau de sécurité adapté aux applications industrielles.



Pour mettre en service la connexion distante des utilisateurs il faut successivement effectuer les étapes suivantes :

- Etape 1 :

Configurer la communication distante. PPTP ou TLS ;

- Etape 2 :

Enregistrer les utilisateurs autorisés dans la «liste d'utilisateurs ».

- Etape 3 :

Définir les droits d'accès de chaque utilisateur.

17.1 Etape 1 : Configuration de la connexion distante

17.1.1 Avantages de la connexion distante

Une connexion distante établie depuis un PC, une tablette ou un smartphone procure les avantages suivants :

- **Identification des utilisateurs distants**
  L’utilisateur distant est identifié au moyen d’un identificateur et d’un mot de passe ou bien encore d’un certificat. L’utilisateur n’est autorisé que s’il a été enregistré dans la liste d’utilisateurs.

- **Connexion transparente**
  S’il y est autorisé par ses droits d’accès, l’utilisateur peut accéder à chaque équipement du réseau distant.

- **Attribution automatique d’une adresse IP du réseau**
  Le PC de l’utilisateur distant est téléporté sur le réseau local. Une fois identifié, son PC reçoit automatiquement une adresse IP du réseau local. Aucune intervention n’est nécessaire dans le PC de l’utilisateur distant.

- **Cryptage des échanges**
  Les connexions distantes permettent de crypter les échanges pour assurer la confidentialité.

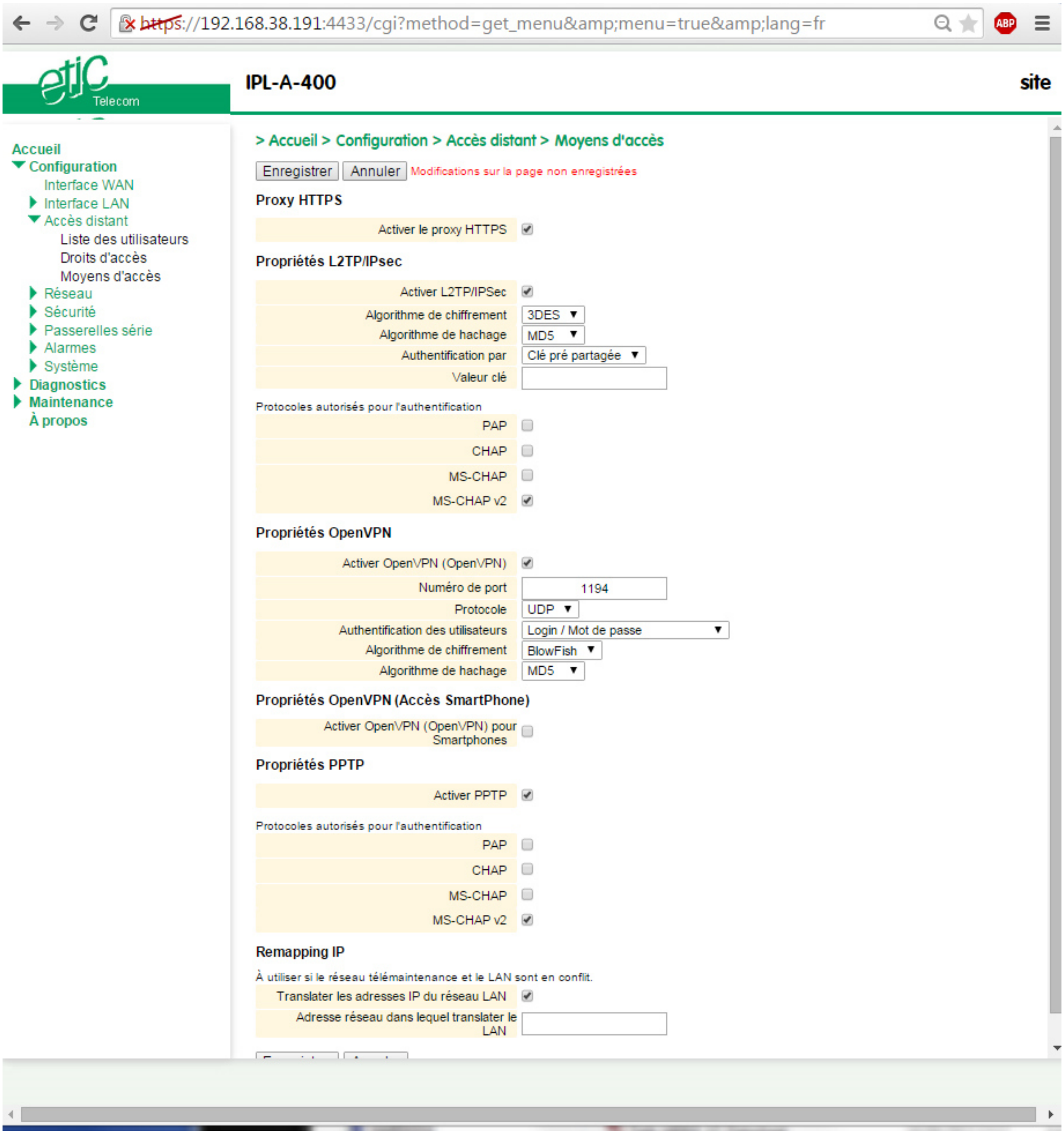
17.1.2 Types de connexions distantes

Quatre types de VPN sont proposés : OpenVPN., PPTP et L2TP/IPSec et HTTPS.

Les quatre types de connexion peuvent co-exister.

Pour paramétrer une connexion distante,

- Sélectionner le menu Configuration > Accès distant > moyen d'accès



17.1.3 Paramétrage d'une connexion distante de type OpenVPN

Une connexion distante OpenVPN établie entre un PC distant et un réseau Ethernet garantt un niveau élevé de sécurité : Authentification, chiffrement, intégrité des données.

Le logiciel M2Me_Secure s'installe sur le PC distant pour constituer une interface de connexion simple et puissante.

Il est aussi possible de paramétrer dans le PC une connexion de type « client OpenVPN ».

Configuration du routeur

- Sélectionner la case à cocher OpenVPN

Paramètres « Numéro de port » et « protocoles » :

Choisir le protocole de transport du VPN (UDP ou TCP) ; UDP est préférable à TCP.

Le N° de port peut être quelconque mais la valeur doit être choisie parmi celles qui sont autorisés sur le réseau du client.

Attention : Le numéro de port utilisé pour l'interconnexion de routeurs par VPN doit être différent du N° de port utilisé pour les connexions d'utilisateurs distants TLS.

Paramètres « Authentification des utilisateurs» :

Si l'on choisit la valeur « Login / mot de passe », l'authentification est réalisée à l'aide de ces deux codes uniquement.

Si l'on choisit la valeur « Login / mot de passe et certificat numérique», la sécurité est renforcée. Le PC distant est authentifié au moyen du certificat enregistré dans le PC et l'utilisateur est identifié au moyen du login et du mot de passe.

Note : dans ce cas, le nom du certificat du PC de l'utilisateur devra être enregistré dans le routeur IPL, dans la fiche de l'utilisateur.

Paramètres « Algorithme de chiffrement» et « Algorithme de hachage » :

Laisser les valeurs par défaut Blowfish et MD5.

Configuration du logiciel M2Me_Secure du PC

- Cliquer l'icône « Menu » puis « Nouveau site ». La fenêtre de paramétrage du site apparaît.
- Sélectionner l'onglet « Général », saisir le nom du site.
- Sélectionner l'onglet « Connexion » ; cocher la case « Ce site est accessible par Internet ».
- Dans le champ « Nom d'hôte ou adresse IP », saisir l'adresse IP permettant d'atteindre le routeur.
- Sélectionner l'onglet « Avancé » ; Choisir le protocole (UDP ou TCP), le N° du port et les algorithmes de cryptage et hachage.

Attention : Ces paramètres doivent avoir la même valeur que ceux sélectionné dans le routeur.

17.1.4 Paramétrage d'une connexion OpenVPN pour smartphone

Il est possible de distinguer l'accès VPN destiné aux PC (voir paragraphe précédent de l'accès destiné aux smartphones.

Cette connexion est de type identique à la connexion OpenVPN du paragraphe précédent mais on la distingue par le N° de port de destination.

- Sélectionner la case à cocher OpenVPN pour smartphone

Paramètres « Numéro de port » et « protocoles » :
Choisir le protocole de transport du VPN (UDP ou TCP) ; UDP est préférable à TCP.
Le N° de port peut être quelconque mais la valeur doit être choisie parmi celles qui sont autorisés sur le réseau du client.

Attention : Le numéro de port utilisé pour l'interconnexion de routeurs par VPN doit être différent du N° de port utilisé pour les connexions d'utilisateurs distants TLS.

Paramètres « Authentification des utilisateurs» :
Si l'on choisit la valeur « Login / mot de passe », l'authentification est réalisée à l'aide de ces deux codes uniquement.

Si l'on choisit la valeur « Login / mot de passe et certificat numérique», la sécurité est renforcée. Le PC distant est authentifié au moyen du certificat enregistré dans le PC et l'utilisateur est identifié au moyen du login et du mot de passe.

Note : dans ce cas, le nom du certificat du PC de l'utilisateur devra être enregistré dans le routeur IPL, dans la fiche de l'utilisateur.

Paramètres « Algorithme de chiffrement» et « Algorithme de hachage » :
Laisser les valeurs par défaut Blowfish et MD5.

17.1.5 Paramétrage d'une connexion distante de type PPTP

Configurer le routeur

- Sélectionner la case à cocher PPTP

Sélectionner le choix PPTP .

Configurer la connexion PPTP dans le PC
Voir procédure en annexe 2.

17.1.6 Paramétrage d'une connexion distante de type L2TP / IPSec

- Sélectionner la case à cocher L2TP / IPSec

Paramètres « Algorithme de chiffrement» et « Algorithme de hachage » :
Laisser les valeurs par défaut Blowfish et MD5.

Paramètres « Authentification des utilisateurs» :
Si l'on choisit la valeur « Login / mot de passe », l'authentification est réalisée à l'aide de ces deux codes uniquement.

Si l'on choisit la valeur « certificat numérique», le PC distant est authentifié au moyen du certificat enregistré dans le PC distant.

Note : Dans ce cas, le nom du certificat du PC de l'utilisateur devra être enregistré dans le routeur IPL, dans la fiche de l'utilisateur.

Paramètres « Valeur clé » :
Saisir la valeur de la clé partagée qui authentifie l'utilisateur distant.

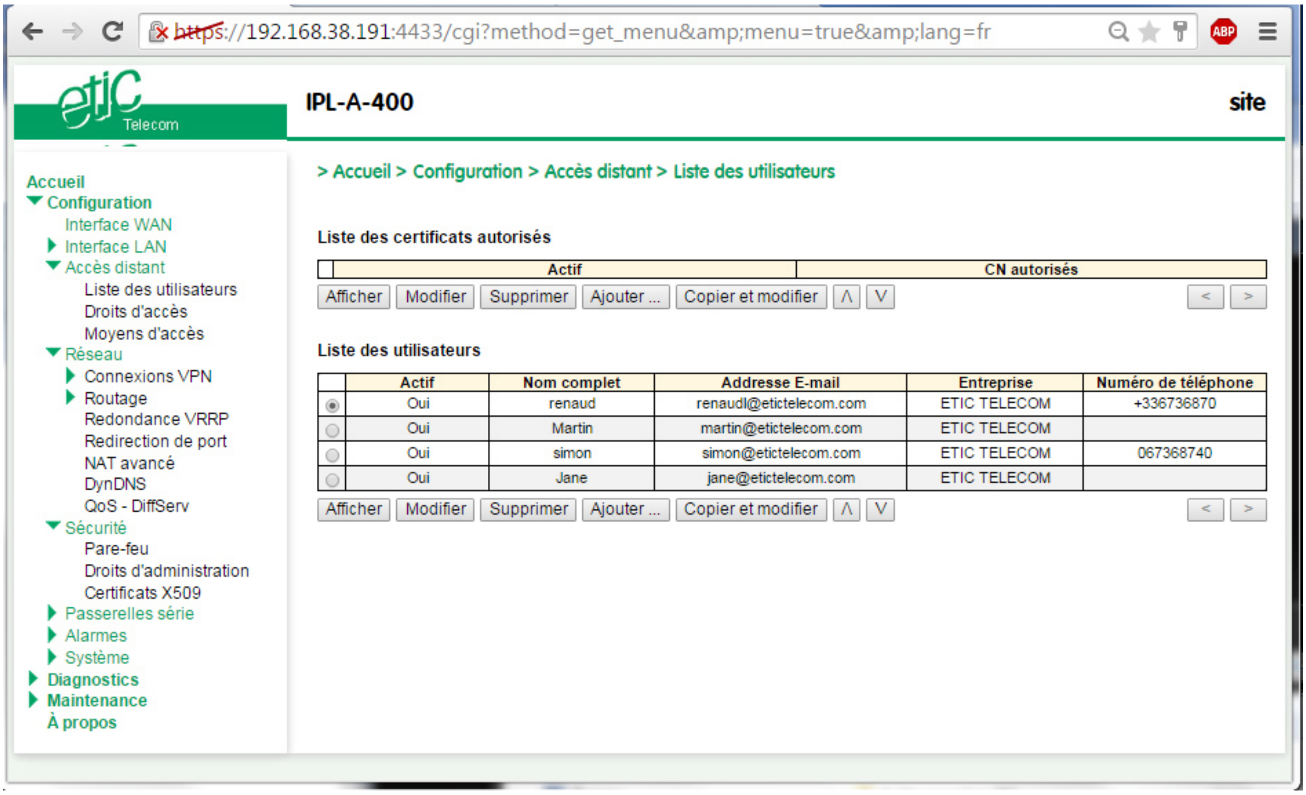
17.2 Etape 2 : Enregistrer les utilisateurs distants autorisés

17.2.1 Présentation

La liste d'utilisateurs du routeur IPL enregistre l'identité de chaque utilisateur distant autorisé à se connecter ainsi que ses paramètres (email…) et ses droits d'accès aux machines du réseau local définis dans le firewall.

Pour accéder à la liste d'utilisateurs,

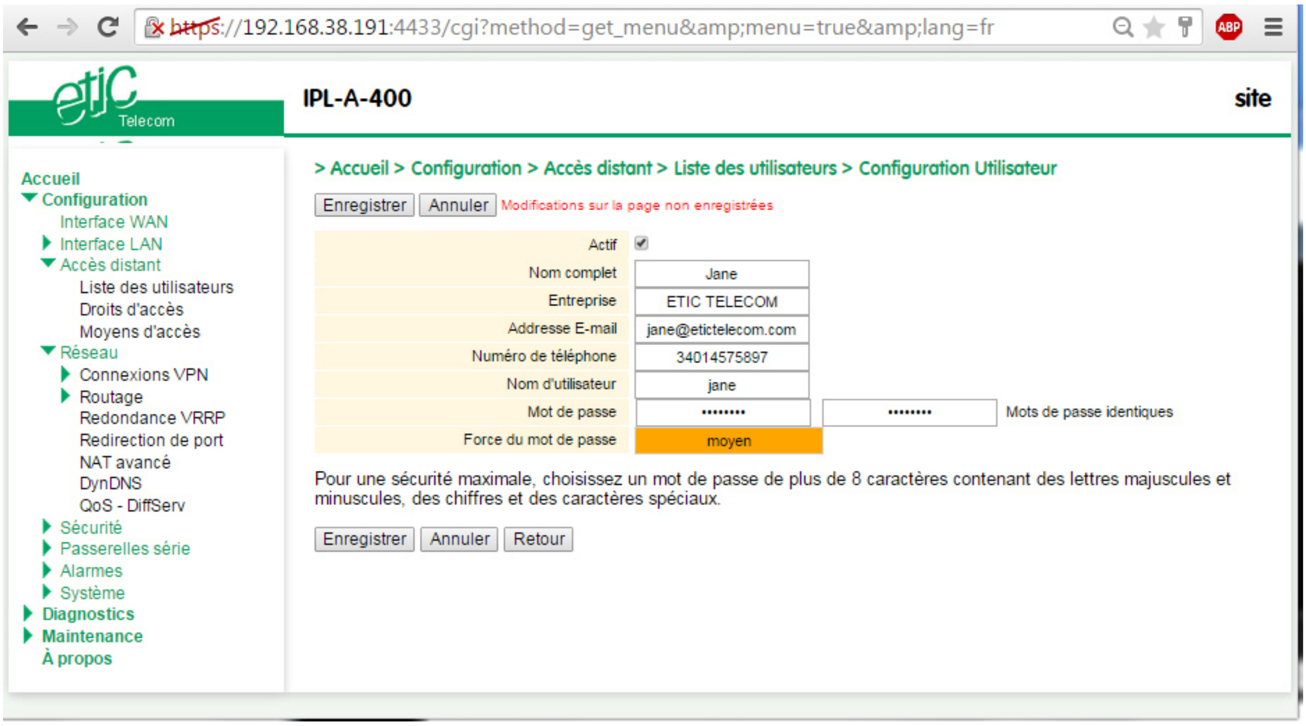
- Sélectionner le menu « Configuration > Accès distant > Liste d'utilisateurs



Note :
A la livraison, pour des raisons de sécurité, aucun utilisateur n'est enregistré.

17.2.2 Définir des utilisateurs

- Cliquer sur le bouton « Ajouter » ; la fiche utilisateur est affichée.



Case à cocher « Actif » :
Elle permet de retirer temporairement un utilisateur de la liste.

Paramètre « Nom complet » :
C'est le libellé qui apparaît dans le premier champ de la liste des utilisateurs autorisés. Il permet en particulier de garder la trace de chaque connexion de l'utilisateur dans le journal.

Paramètres « Email » et « N° de téléphone » :
L'adresse mail permet l'émission d'un email d'alarme.

Remarque : le champ N° de téléphone est réservé pour des usages ultérieurs.

Paramètres « Nom d'utilisateur » et « mot de passe » :
Ce sont deux codes différents attribués à chaque utilisateur. Lorsqu'il se connecte à distance, il doit saisir ces deux codes dans les champs correspondants de la fenêtre de CONNEXION DISTANTE.

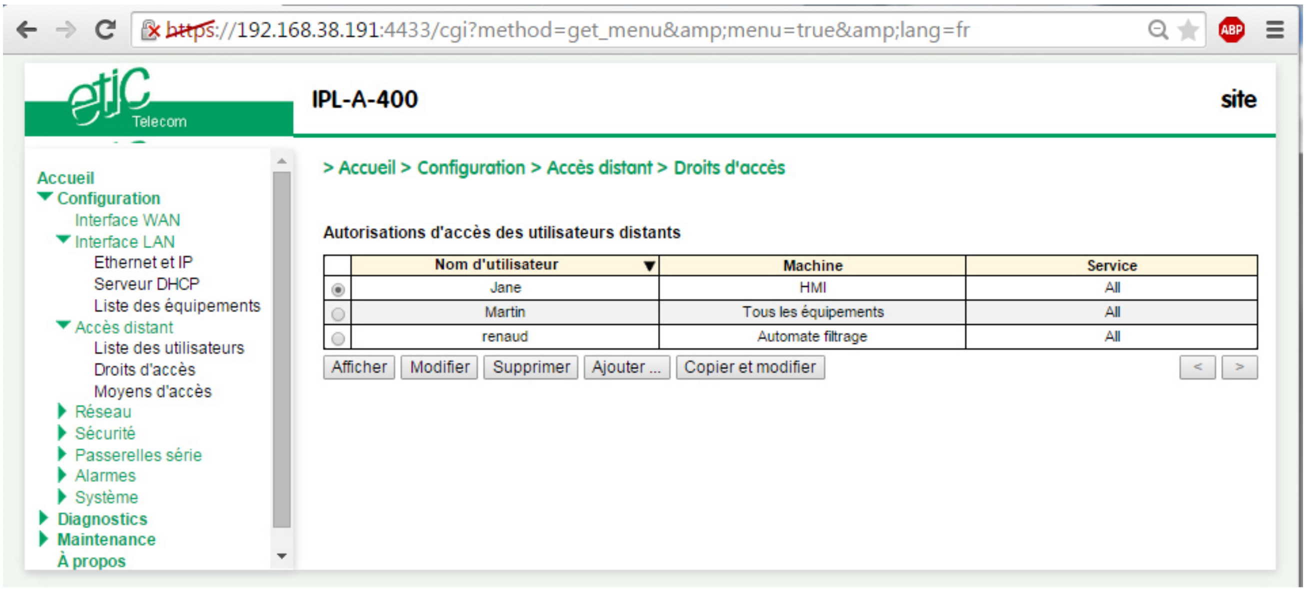
17.3 Etape 3 : Définir les droits d'accès des utilisateurs

Il est possible de définir les équipements auxquels chaque utilisateur peut accéder.

Au préalable, il faut définir la liste des machines du réseau qui sont accessibles à distance (voir menu Interface LAN > Liste des équipements).

Pour définir les droits d'accès d'un utilisateur

- Sélectionner le menu Configuration > Droits d'accès, le tableau des droits s'affiche.



- Cliquer le bouton « Ajouter » ; puis sélectionner un utilisateur dans la liste puis luis attribuer un équipement dans la liste pour autoriser l'accès à cet équipement.

18 Portail sécurisé (HTTPS) pour smartphone, tablette ou PC

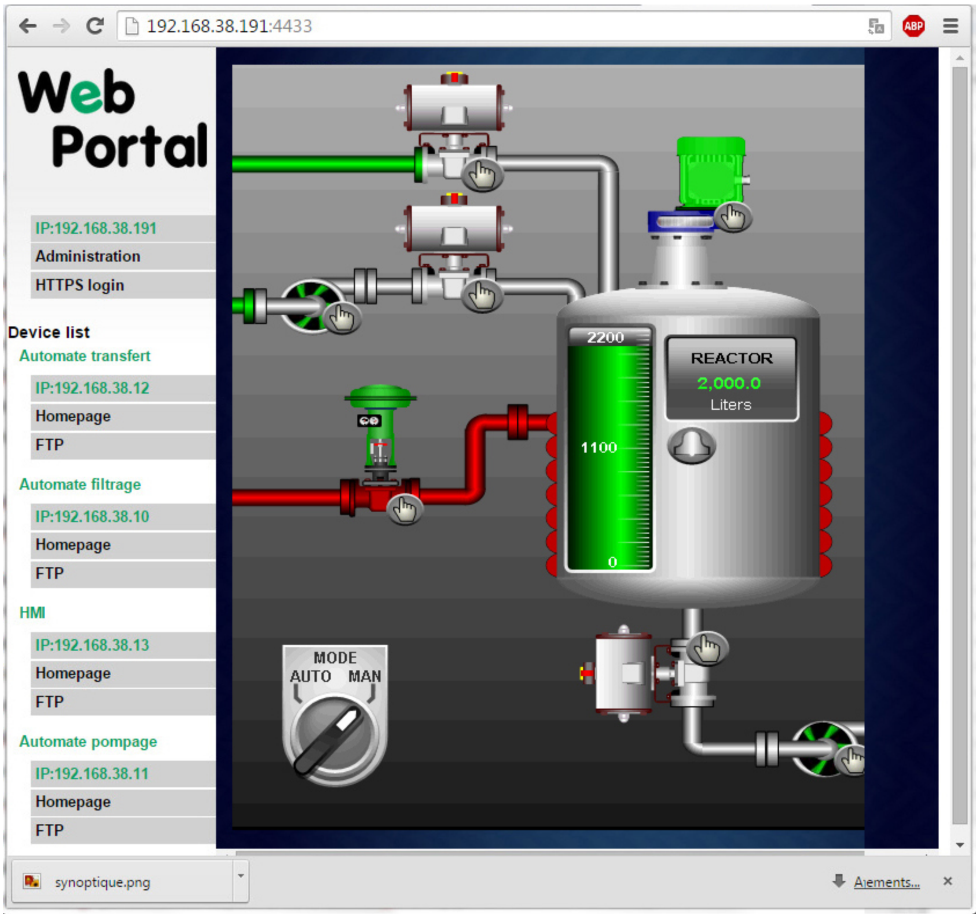
18.1 Présentation

Le portail sécurisé est une page web affichée par le routeur lorsqu'un utilisateur distant se connecte au routeur au moyen d'un simple navigateur en mode sécurisé HTTPS.

La page « Portail » affiche la liste des équipements accessibles à l'utilisateur selon ses droits d'accès.

Il suffit de cliquer sur l'équipement souhaité et les pages web du serveur web embarquées dans cet équipement s'affichent.

Conjuguée à une alarme SMS ou email, le portail web est particulièrement adapté à la télé-exploitation au moyen de smartphone.



18.2 Configuration

Pour activer la fonction portail web HTTPS et y donner accès par le réseau LAN,

- Sélectionner le menu Configuration > Accès distant > Moyen d'accès
- Cocher la case « Activer le proxy HTTPS ».

Pour y donner en plus accès par l'Internet (WAN),

- Sélectionner le menu Configuration > Sécurité > Droits d'administration
- Cocher la case « Utiliser HTTPS pour la configuration »
- Cocher la case « Activer l'accès par le WAN ».

Note importante :

Lorsque le portail HTTPS est activé, le serveur de configuration du routeur est remplacé par le portail web ; Cependant, le serveur de configuration reste accessible mais, il faut préciser le N° de port :

Accès	Par l'Internet	Par le LAN
Portal Web HTTPS :	https://adr. IP Internet	https://adr. IP LAN du routeur
Serveur de configuration HTTPS du routeur	https://adr. IP Internet : 4433 ou adr. IP Internet :8080 avec login et PWD	Adr. IP LAN du routeur

18.3 Accéder au portail HTTPS par l'Internet

Pour accéder au portail web HTTPS par l'Internet,

- Lancer le navigateur
- Entrer l'adresse publique Internet du routeur : https : // « adresse IP Internet du routeur »
- Saisir le nom et le mot de passe d'un utilisateur enregistré dans la liste d'utilisateurs.

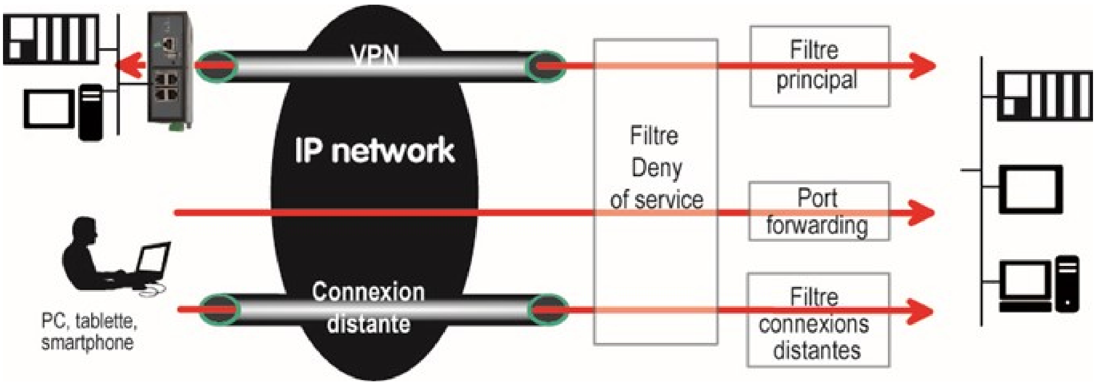
La page d'accueil du portail HTTPS s'affiche ; elle n'affiche que les équipements autorisés à l'utilisateur.

19 Configuration du pare-feu

19.1 Présentation du pare-feu

Le pare-feu a pour but de filtrer les échanges de trames IP entre l'interface WAN et l'interface LAN pour protéger les équipements connectés au réseau LAN.

Sa structure est résumée ci-dessous :



Il comporte trois parties :

- **Le filtre principal**
  Il filtre les trames IP en fonction de l'adresse IP et du port source et de l'adresse IP et du port destination.

  Ce filtrage s'applique aux trames véhiculées dans les VPN ou hors des VPN.

  Pour une meilleure organisation, il comporte deux filtres séparés :
  Le filtre qui agit sur les trames IP véhiculées dans les VPN
  Le filtre qui agit sur les trames IP véhiculées hors des VPN

Le filtre principal agit sur toutes les trames sauf celles qui sont véhiculées dans les connexions d'utilisateurs distants qui sont traitées par le filtre d'utilisateurs distants (voir ci-dessous).

Pour distinguer une connexion d'utilisateur distant de type OpenVPN d'un tunnel OpenVPN établi entre routeurs, le routeur détecte le N° de port : Si le N° de port détecté est le N° déclaré pour une connexion d'utilisateurs distants), le filtre des connexion d'utilisateurs s'appliquera et pas le filtre principal..

Notes :
On veillera donc à choisir un N° de port différent pour les connexions OpenVPN d'Utilisateur distant et les connexions OpenVPN entre routeurs.

La fonction dite de redirection de port qui renvoie le trafic destiné au routeur sur l'interface WAN (Internet) vers une adresse IP particulière de l'interface LAN sur le critère de N° de port, n'est pas soumise au filtre principal.

- **Les filtres d'«Utilisateur distant »**
  Ils permettent d'autoriser ou d'interdire l'accès à chaque équipement connecté à l'interface LAN en fonction de l'identité de l'utilisateur distant (Login et mot de passe et éventuellement certificat) lorsqu'il se connecte au moyen de la connexion distante PPTP OpenVPN ou L2TP/IPSec..

  Par exemple, on peut attribuer à l'utilisateur de login « admin » et de mot de passe « admin » un filtre bloquant toutes les trames issues de son PC sauf celle qui sont adressées à un équipement particulier de l'interface LAN.

Note :
La configuration de ce filtre est réalisée dans le menu Configuration > Accès distant > Droits d'accès

- **Le filtre de « déni de Service »**

Le filtre de déni de service (DoS) protège les équipements de l'interface LAN contre les attaques par saturation pouvant provenir de l'interface WAN : Ping de la mort, SYN flood
Ce filtre est prédéfini et n'est pas configurable par l'utilisateur. Il toujours opérationnel sur l'interface WAN.

19.2 Filtre principal

19.2.1 Présentation

- **Organisation**

Le filtre principal comporte deux parties

La première partie est intitulée **« Règles pour le trafic WAN »**
Elle a pour but de définir le filtrage à apporter aux trames IP non transportées dans un VPN.

Elle définit la politique par défaut et le tableau de règles de filtrage.
Chaque ligne du tableau est une règle de filtrage qui autorise ou interdit un type de trames IP.

La seconde partie est intitulée **« Règles pour le trafic VPN »**
Elle a pour but de définir le filtrage à apporter aux trames IP transportées dans un VPN.

Elle a la même forme que la première partie.

- **Politique par défaut :**

C'est l'action qui sera appliquée à une trame qui n'est conforme à aucune règles du tableau.

On considère séparément les deux directions de trafic car on peut souhaiter que la décision prise soit différente selon qu'un paquet provient du LAN ou du WAN.

On peut souhaiter, par exemple que la politique par défaut interdise le routage « WAN vers LAN » mais autorise le routage « LAN vers WAN ».

La politique par défaut prudente consiste à interdire le trafic WAN vers LAN et éventuellement LAN vers WAN ; de cette façon, toute trame qui ne se conforme pas à l'une des règles du filtre est bloquée.
En effet, supposons que la politique par défaut consiste à autoriser le trafic WAN vers LAN ; alors tout flux IP qui ne serait conforme à aucune des règles du filtre principal, serait routée vers le LAN.

- **Tableau de règles de filtrage**

Chaque ligne est une règle de filtrage.

Chaque règle définit une action (autoriser ou interdire) associée à un flux IP défini par les différents champs de la ligne de règle :

Direction (« LAN vers WAN » ou « WAN vers LAN »),
protocole (TCP, UDP…),
@IP et port source
@IP et port destination

Voici un exemple de filtre qui autorise deux équipements du réseau WAN (192.168.2.X) à accéder à un équipement particulier du réseau LAN. Tout autre flux du WAN vers le LAN est interdit.

Politique par défaut : LAN -> WAN : Autoriser - WAN -> LAN : interdire						
Direction	**Action**	**Protocole**	**@ IP source**	**port source**	**@IP destination**	**port dest**
WAN->LAN	Autoriser	any	192.168.2.1	any	192.168.1.12	any
WAN->LAN	Autoriser	TCP	192.168.2.2	any	192.168.1.12	502

- **Fonctionnement**

Lorsque le firewall reçoit une trame IP véhiculée dans le VPN, il applique la politique et les règles du filtre « Trafic VPN ».

Lorsque le firewall reçoit une trame IP véhiculée hors du VPN, il applique la politique et les règles du filtre « Trafic WAN ».

Il vérifie successivement la conformité aux règles de filtrage.
Si la trame n'est pas conforme à la première règle, elle est soumise à la suivante et ainsi de suite.
Dès qu'elle est conforme à une règle du tableau, le firewall lui applique l'action associée (autoriser ou interdire).
Si la trame n'est conforme à aucune règle, la politique par défaut lui est appliquée (autoriser ou interdire).

Note :

A la livraison, le filtre principal est réglé de la façon suivante :

Le trafic véhiculé dans les VPN est autorisé sans restriction.

Le trafic véhiculé hors des VPNs est limité :
    Le trafic à l'initiative d'un équipement du LAN vers le WAN est autorisé.
    Le trafic à l'initiative d'un équipement du WAN vers le LAN est interdit

20 Configuration des passerelles série

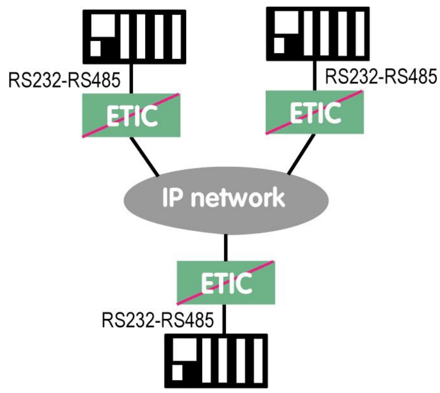
20.1 Présentation des types de passerelles

Certains modèles du routeur comportent 1 ou 2 liaisons série : RS232, RS232, RS485 ou RS422.

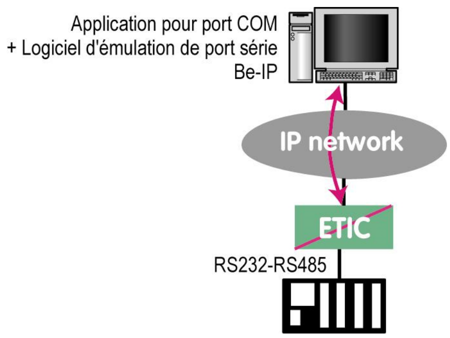
Une passerelle peut être affectée à chaque liaison série.

Une passerelle série permet d'utiliser le réseau IP pour faire communiquer des équipements série entre eux ou bien avec des équipements IP.

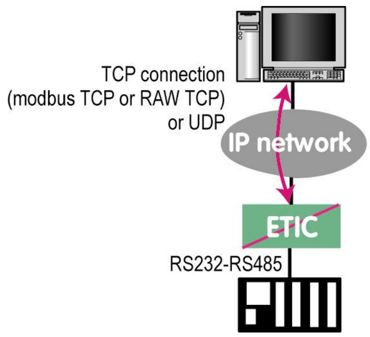
- Communication entre équipements à interface série



- Communication avec une application sur PC windows prévue initialement pour dialoguer par la liaison série.
Le logiciel d'émulation de port COM Be-IP est une passerelle software qui permet d'utiliser sur un réseau IP un logiciel d'application conçu initialement pour communiquer sur **une liaison série.**



- Communication avec application sur PC capable d'empaqueter un protocole série dans UDP ou TCP (modbus TCP par exemple)



Pour réaliser les fonctions décrites ci-dessus et s'adapter aux différentes situations qu'il est possible de rencontrer, différents types de passerelles sont proposées :

1er type : Passerelle Modbus
Ce type de passerelle permet de raccorder à la liaison série un équipement modbus maître, ou bien des équipements modbus esclaves ou bien les deux, pour les faire communiquer avec d'autres équipements modbus TCP ou modbus asynchrones connectés au réseau IP.

2eme type : Passerelle transparente point à point
Cette passerelle est appelée RAW client ou RAW serveur ; elle permet de relier un équipement série à un autre équipement série utilisant le même type de passerelle à travers le réseau IP.

3eme type : Passerelle de diffusion vers un ensemble d'abonnés (RAW UDP)
Cette passerelle est appelée RAW UDP client ou RAW UDP serveur ; elle permet de relier entre eux un groupe d'équipements série et un ensemble d'équipements du réseau IP désignés lors de la configuration.
Cette solution est très simple de mise en œuvre ; on désigne chaque correspondant par son adresse IP; les données série sont envoyées sous forme de datagrammes UDP à chaque correspondant IP enregistré ; réciproquement, les données reçues par la passerelle au N° de port convenu, sont transmises sur la liaison série.

4eme type : Passerelle Telnet
Cette passerelle permet à un PC sur le réseau IP et équipé d'un logiciel client Telnet de se connecter à un équipement serveur Telnet raccordé à la liaison série.
Le débit et le format de la liaison série peuvent être pilotés selon la recommandation RFC2217.

20.2 Passerelle Modbus

La passerelle Modbus permet de connecter des équipements série RS232-RS485 esclaves ou maître à un ou plusieurs équipements modbus TCP (clients ou serveurs selon le cas) connectés au réseau IP.

20.2.1 Définitions

Un client TCP MODBUS est un équipement connecté au réseau IP et capable de transmettre une requête Modbus (= question ; par ex. demande de lecture ou d'écriture) à un autre équipement du réseau appelé serveur TCP MODBUS qui lui répondra.

Le client est l'équivalant d'un maître Modbus, mais plusieurs clients peuvent poser des questions au même serveur.

Un serveur TCP MODBUS est un équipement connecté au réseau IP et capable de répondre à une requête Modbus posée par un autre équipement du réseau appelé client TCP MODBUS.

Le serveur est l'équivalant d'un esclave Modbus ; mais un serveur peut répondre à plusieurs clients.

Un maître Modbus est un équipement connecté à la liaison série RS232 ou RS485 et capable de poser une requête Modbus à un autre équipement du réseau appelé esclave MODBUS.

Un esclave Modbus est un équipement connecté à la liaison série RS232 ou RS485 et capable de poser une question Modbus à un autre équipement du réseau qui est appelé esclave MODBUS.

Adresse Modbus : Elle code entre 0 et 255 le destinataire d'une requête modbus adressée à un serveur modbus (réseau IP) ou à un esclave modbus (liaison série).

Attention : Ne pas confondre adresse modbus et adresse IP.
Pour plus de concision le mot « adresse » est souvent remplacé par le signe @ dans la suite du texte.

20.2.2 Choix de la passerelle Client ou de la passerelle Serveur

- Pour connecter des équipements «série» esclaves modbus à un ou plusieurs équipements TCP modbus client, sélectionner le menu passerelle « Modbus serveur ».

- Pour connecter un équipement «série» maître modbus à un ou plusieurs équipements TCP modbus serveur, sélectionner le menu passerelle « Modbus client ».

20.2.3 Affectation d'une passerelle modbus à un port série

La passerelle modbus client (respectivement serveur) peut être affectée au port série COM1 ou au port série COM2.

Si l'on veut affecter la passerelle série Modbus client (respectivement modbus serveur) aux ports COM1 et COM2 à la fois, deux numéros de **ports TCP différents** doivent être paramétrés.

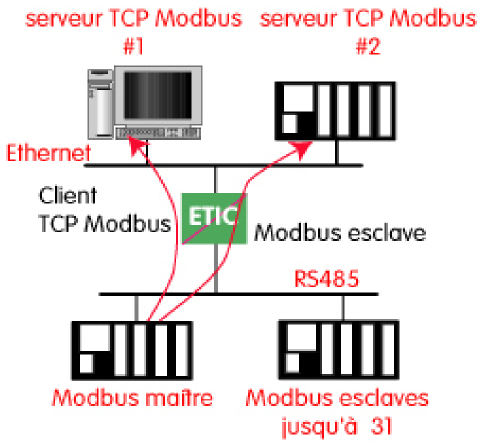
La passerelle modbus client peut être affectée à un port série (COM1 par ex) tandis que la passerelle Modbus serveur est affectée à l'autre port série (COM2 par ex.).

20.2.4 Passerelle modbus client

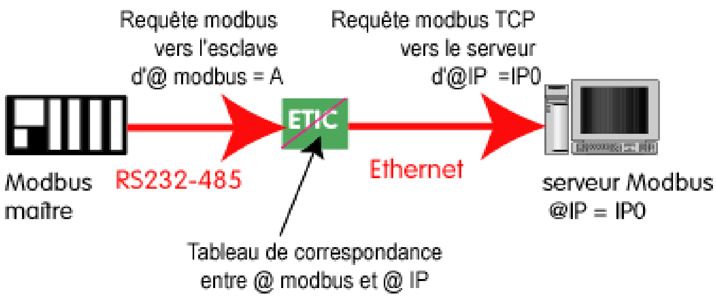
La passerelle modbus client permet la connexion d'un maître modbus sur la liaison série.

Plusieurs serveurs TCP modbus peuvent être adressés sur le réseau iP.

D'autres esclaves peuvent être connectés à la liaison série.



Principe de la passerelle modbus Client :
Pour adresser un serveur TCP modbus sur le réseau IP, on configure une table de correspondance entre une @ modbus esclave et une @ IP ; ainsi, lorsque le maître modbus transmet une requête à destination de l'esclave d'@ modbus A, le tableau de correspondance permet de transmettre cette requête à l'@ IP correspondant à l'@ A .
De plus, le champ adresse modbus de la trame modbus TCP prend la valeur A.
Le tableau de correspondance peut comporter 32 lignes permettant ainsi à un maître modbus d'adresser 32 serveurs sur le réseau IP.



Configuration de la passerelle modbus Client :

- Sélectionner le menu « **Passerelle IP-RS** », puis cliquer le menu « **Modbus** » puis « **Modbus client** ».
- Cocher « activer la passerelle ».

Paramètre « Sélection du port » :
Choisir la liaison série 1 ou 2 du routeur.

Bouton « COM » :
Permet de configurer les paramètres débit et format de la liaison série.

Paramètre « Protocole Modbus » :
Sélectionner RTU (hexadécimal) ou ASCII selon le besoin.

Paramètre « Temps inter caractères » :
Fixe le temps maximum admissible entre caractères des réponses de l'esclave modbus.

Paramètre « Timeout d'inactivité sur TCP » :
Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de requêtes modbus reçues du réseau IP.

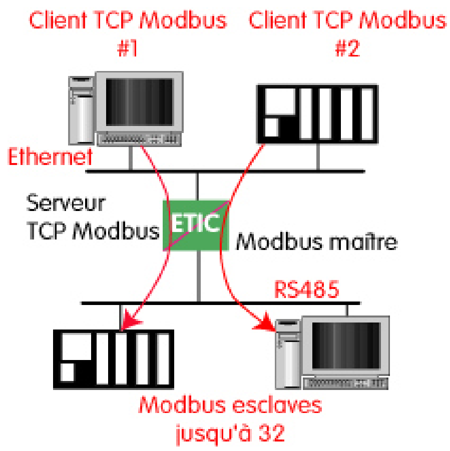
Paramètre « Numéro du port TCP » :
Fixe le N° du port TCP à utiliser. Le N° de port modbus par défaut est 502.

Tableau de correspondance :
Le tableau de correspondance permet de faire correspondre une adresse d'esclave modbus et une adresse IP.

20.2.5 Passerelle modbus serveur

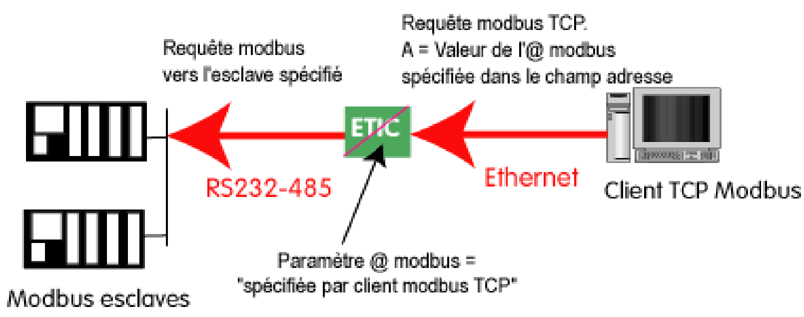
La passerelle permet la connexion d'esclaves modbus sur la liaison série.

32 esclaves, au maximum, peuvent être connectés au port RS485.

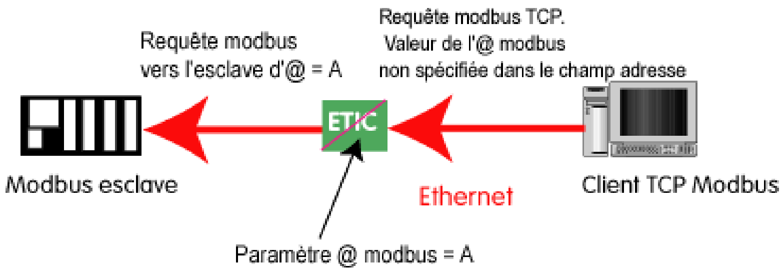


Un client TCP modbus adresse une requête TCP modbus à la passerelle ;
La passerelle se comporte en maître sur la liaison série.
Elle « répète » la requête sur la liaison série ; l'adresse de la requête émise sur la liaison série est,

- soit l'adresse contenue dans le champ d'adresse modbus TCP, dans ce cas, plusieurs esclaves peuvent être adressés sur la liaison série :



- soit une adresse fixe configurée dans la passerelle (voir ci-dessous) ; dans cas, un seul esclave peut être adressé sur la liaison série :



Attention : Plusieurs client TCP modbus peuvent adresser des requêtes aux esclaves de la liaison série. Néanmoins, on prendra garde à ne pas saturer la liaison série puisque son débit est bien inférieur à celui d'Ethernet.

Configuration de la passerelle Modbus serveur :

- Sélectionner le menu « **Passerelle IP-RS** », puis cliquer sur « **Modbus** », puis « **Modbus serveur** ».
- Cocher « activer la passerelle ».

Paramètre « Sélection du port » :
Choisir la liaison série 1 ou 2 du routeur.

Bouton « COM » :
Permet de configurer les paramètres débit et format de la liaison série.

Paramètre « Protocole Modbus » :
Sélectionner RTU (hexadécimal) ou ASCII selon le besoin.

Paramètre « Activer la fonction proxi-cache » :
Si cette fonction est active, une requête n'est adressée à un esclave que si la même requête ne lui a pas été adressée depuis le temps fixé par le paramètre « rafraîchissement du cache.

Paramètre « Rafraîchissement du cache » :
Fixe le délai minimum entre deux requêtes identiques adressées au même esclave.

Paramètre « Temps d'attente réponse esclave » :
C'est le délai d'attente de réponse à la requête adressée à un esclave.

Paramètre « Nombre de réitérations » :
Fixe le nombre de réitérations d'une requête modbus par le routeur en cas de non réponse de l'esclave modbus.

Paramètre « Temps inter caractères » :
Fixe le temps maximum admissible entre caractères des réponses de l'esclave modbus.

Paramètre « Adresse esclave Modbus » :
Si la valeur « spécifiée par le client modbus » est sélectionnée, la passerelle utilise l'adresse modbus spécifiée par le client modbus pour adresser l'esclave modbus de la liaison série ; on peut ainsi adresser jusqu'à 32 esclaves de la liaison série.

Si l'on sélectionne une valeur particulière (entre 1 et 255), la passerelle adresse toutes les requêtes au N° d'esclave sélectionné ; on ne peut interroger qu'un seul esclave sur la liaison série.

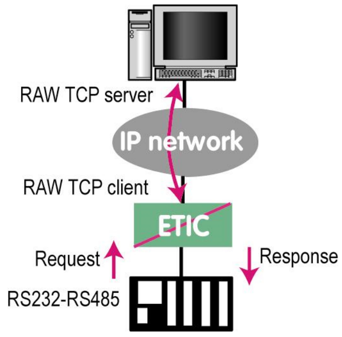
Paramètre « Time out d'inactivité sur TCP » :
Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de requêtes modbus reçues du réseau IP.

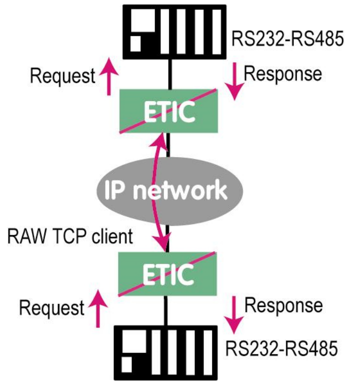
Paramètre « Numéro du port TCP » :
Fixe le N° du port TCP à utiliser ; le port par défaut est 502.

20.3 Passerelle « TCP RAW »

20.3.1 Passerelle « TCP RAW » client

Elle permet de raccorder un équipement se comportant en « maître » sur la liaison RS232 / RS485





Configuration :

- Cliquer le menu « passerelle » puis« Transparent ». Puis « raw client»
- Cocher « activer la passerelle ».

Paramètre « Taille du buffer de réception RS232/485» (valeur 1 à 1024) :
Fixe la taille maximum, en octets, d'un bloc transmis vers le réseau IP.

Paramètre « Timeout fin de trame RS232/485» (valeur 10 à 500 ms) :
Fixe délai de silence maximum après lequel le buffer de caractères reçus de la liaison RS232-RS485 est transmis vers le réseau IP.

Paramètre « Timeout d'inactivité sur socket TCP» (valeur 0 à 5 mn) :
Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de caractères reçus du réseau IP ou de la liaison série.

Paramètre « Numéro du port TCP » :
Fixe le N° du port TCP à utiliser.
Attention : Si 2 passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même N° de port TCP.

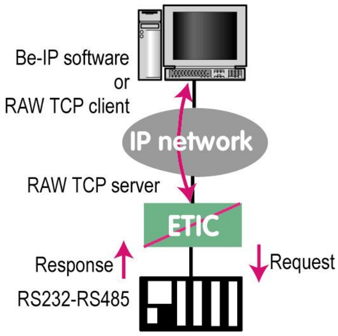
Paramètre « Adresse IP du serveur Raw TCP » :
Fixe l'adresse IP à laquelle sont transmis les caractères reçus de la RS232 / RS485 (c'est l'adresse du serveur RAW).).

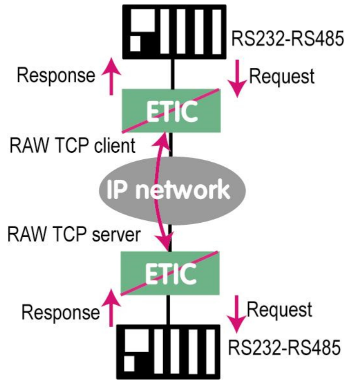
20.3.2 Passerelle « RAW serveur »

Elle permet de raccorder des équipements « esclaves » sur la liaison RS232-RS485.

L'équipement de la liaison série peut ainsi communiquer avec un PC Client RAW TCP.

La passerelle « RAW serveur » peut en particulier être utilisée avec profit en association avec le logiciel **Be IP** d'etic dans le cas où il faut faire communiquer par un réseau IP





Configuration de la passerelle RAW serveur :

- Cliquer le menu « passerelle » puis« Transparent ». Puis « raw serveur»
- Cocher « activer la passerelle » puis régler les paramètres :

Paramètre « Taille du buffer de réception RS232/485» (valeur 1 à 1024) :
Fixe la taille maximum, en octets, d'un bloc transmis vers le réseau IP.

Paramètre « Timeout fin de trame RS232/485» (valeur 10 à 500 ms) :
Fixe délai de silence maximum après lequel le buffer de caractères reçus de la liaison RS232-RS485 est transmis vers le réseau IP.

Paramètre « Timeout d'inactivité sur socket TCP» (valeur 0 à 5 mn) :
Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de caractères reçus du réseau IP ou de la liaison série.

Paramètre « Numéro du port TCP » :
Saisir le N° du port TCP à utiliser.

Attention : Si 2 passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même N° de port TCP

20.4 Passerelle “RAW UDP”

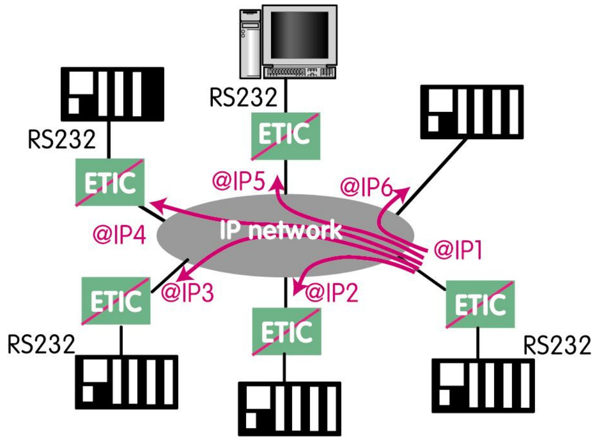
20.4.1 Présentation

Cette passerelle permet de relier un ensemble d’équipements série ou IP, au travers d’un réseau IP.

Les destinataires sont désignés dans une liste établie par configuration.

Cette solution est très simple de mise en œuvre : On désigne chaque correspondant par son adresse IP; les données RS232 sont envoyées sous forme de trames IP adressées individuellement à chaque correspondant enregistré.

.



20.4.2 Configuration

Sélectionner le menu « passerelle » puis « Transparent » puis « Raw UDP »

Cocher « activer » puis régler les paramètres ci-dessous :

Paramètre « Taille du buffer de réception RS232/485» (valeur 1 à 1024) :
Fixe la taille maximum, en octets, d’un bloc transmis vers le réseau IP.

Paramètre « Timeout fin de trame RS232/485» (valeur 10 ms à 5 sec) :
Fixe délai de silence maximum après lequel le buffer de caractères reçus de la liaison RS232-RS485 est transmis vers le réseau IP.

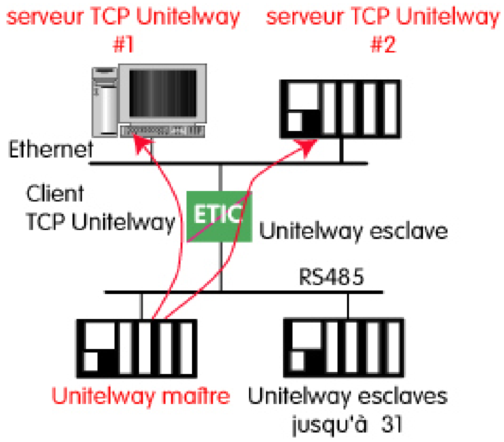
Paramètre « Numéro du port UDP » :
Fixe le N° du port UDP à utiliser permettant de recevoir les données d'un ou plusieurs équipements sur le réseau.

Attention : Si 2 passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même N° de port UDP.

Paramètre Liste de « Destinations » :
Transmettre automatiquement les caractères reçus de la RS232 / RS485 vers les destinations indiqués : pour un équipement maître (ou client), renseigner tous les équipements esclaves. Pour un équipement esclave (ou serveur), renseigner l'équipement maître.
Un équipement est défini par une adresse IP et un port. Vérifier que le port correspond au champ "Numéro du port UDP" configuré dans la passerelle "Raw UDP" de l'équipement distant.

20.5 Passerelle Unitelway

La passerelle Unitelway permet de connecter un automate série maître unitelway à un réseau IP.
Elle permet en particulier de réaliser la fonction de télémaintenance d'automates Schneider Electric RS485 via un réseau IP.



- **Cliquer le menu Unitelway**
- **Cocher « activer la passerelle ».**

Désigner l'adresse Xway de l'automate maître et celle des automates esclaves éventuellement raccordés à l'interface RS485.

21 Passerelle USB

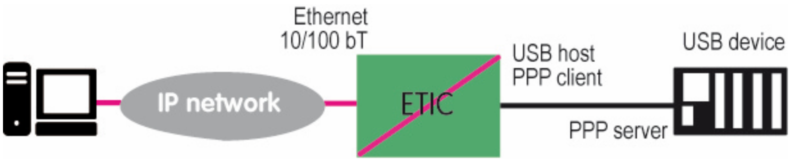
Attention : L'interface USB ne peut pas être utilisé à la fois pour la connexion d'un modem 3G USB (fonction de secours) et pour la fonction de passerelle USB.

21.1 Principe

Elle permet à un ou plusieurs équipements du réseau Ethernet d'échanger des données avec un équipement à interface USB connecté au routeur IPL.

Sur l'interface USB, le routeur IPL se comporte en client PPP.

L'équipement connecté au routeur IPL par l'interface USB se comporte en serveur PPP.



Adresse IP de destination : Cas principal
Un équipement connecté au réseau Ethernet et qui veut transmettre des données à l'équipement connecté à l'interface USB doit adresser les données à l'adresse IP spécifique attribuée à la passerelle USB.
(voir configuration).

Adresse IP de destination : cas du protocole MODBUS :
Si aucune adresse spécifique n'est attribuée à la passerelle USB, la passerelle transfère uniquement vers l'interface USB le trafic Modbus TCP dans le port 502 adressé à l'adresse IP de l'interface LAN du routeur.

21.2 Configuration

- Sélectionner le menu « Configuration » puis « Passerelle USB ».

Case à cocher « Activer» :
Cocher cette case.

Case à cocher « Utiliser une Adresse IP spécifique » :
Cocher cette case pour permettre l'enregistrement d'une adresse IP spécifique de la passerelle USB ; dans ce cas, les données transmises à cette adresse spécifique sont transmises sur l'interface USB quel que soit le N° du port de destination.

Paramètre « Adresse IP spécifique » :
Enregistrer l'adresse IP spécifiquement attribuée à la passerelle USB.

Case à cocher case "Autoriser l'accès depuis l'interface WAN » :
Il est nécessaire de sélectionner cette case si l'équipement est connecté au réseau Ethernet de l'Interface WAN.

Si le PC est connecté par un VPN, par exemple, ou bien dans tout autre cas, il n'est pas nécessaire de cocher cette case.

22 Fonctions avancées

22.1 Ajouter un certificat

Pour établir un tunnel VPN, le routeur IPL peut s'authentifier au moyen de certificat.
Cette solution procure un niveau élevé de sécurité.

Le routeur est livré avec un certificat X509 au format PKC#12 délivré par ETIC TELECOM ; cependant, il est possible d'ajouter un ou plusieurs autres certificats qui pourront être sélectionnés à la place du certificat initial.

Ces certificats peuvent être introduits soit en format PKCS#12 avec mot de passe ou en en format PEM.

Un seul certificat peut être actif à la fois.

Attention : les certificats du routeur client VPN et du routeur serveur VPN doivent avoir été délivrés par la même autorité de certification.

Pour ajouter un certificat,

- Sélectionner Configuration > Sécurité > Certificats.
- Cliquer le bouton ajouter.
- Sélectionner le type de certificat (PKC#12 ou PEM).
- Sélectionner le certificat actif parmi la liste des certificats enregistrés.

22.2 Programmation des alarmes

22.2.1 Alarmes SNMP

Le routeur dispose d'un agent SNMP qui supporte la MIB-II standard et l'envoi de TRAP sous certaines conditions.

Pour enregistrer les paramètres de fonctionnement du gestionnaire SNMP vers lequel les traps doivent être transmis,

- Sélectionner Configuration > Système.

Case à cocher « Activer » :
Si cette case est cochée l'agent SNMP est lancé.

Paramètre « Adresse IP du premier gestionnaire SNMP » :
Ce paramètre enregistre l'adresse IP du gestionnaire SNMP vers lequel les TRAP SNMP doivent être envoyés.

Paramètre « Adresse IP du second gestionnaire SNMP » :
Les traps SNMP peuvent être transmis vers un second serveur SNMP.
Ce paramètre enregistre l'adresse IP de ce second serveur.

Paramètre « version du protocole SNMP » :
Choisir dans la liste la version du protocole SNMP à utiliser.

Paramètre « Nom de communauté » :
C'est nom partagé entre chaque agent et le manager SNMP.
L'agent SNMP ne répond qu'aux requêtes d'un manager qui s'identifie par ce nom.

Paramètres « Nom du système » et « Localisation du système » :
Ces deux paramètres permettent au gestionnaire SNMP d'identifier l'origine des traps.
Saisir les chaînes de caractères qui identifieront le routeur ; leur valeur est au choix.

Case à cocher « Surveiller le statut du backup OpenVPN » :
Le serveur VPN peut surveiller via SNMP l'état des VPN principaux et backup de ses clients.
Il utilise ces données pour afficher un tableau récapitualtif dans la page diag/openvpn.

22.2.2 Alarme e-mail

Un email peut être transmis Lorsque l'entrée TOR du routeur IPL (située sur le bornier à vis) change d'état, une alarme peut être envoyée, sous forme d'un e-mail.

Paragraphe description de l'alarme

Paramètre « Activer l'alarme par email » :
Si cette case est cochée, une alarme par e-mail est émise lorsque l'entrée TOR N° 1 change d'état.

Paramètre « Source de l'alarme » :
Ce paramètre permet de déterminer le ou les changements d'état qui provoquent l'alarme :

Passage à l'état fermé de l'entrée TOR
Passage à l'état ouvert de l'entrée TOR
Passage à l'état fermé ou ouvert de l'entrée TOR
VPN connecté ou déconnecté

Choisir la source dans la liste.

Paramètre « Destinataire de l'alarme » :
Entrer l'adresse mail du destinataire du mail.

Paramètre « Objet » :
Entrer l'objet du mail ; par exemple « Alarme routeur de Grenoble ».

Paramètre « Texte à envoyer » :
Entrer le texte du mail d'alarme.

Paragraphe Serveur SMTP

Paramètre « Utiliser le service M2Me pour envoyer les emails » :
ETIC TELECOM entretient un serveur SMTP (mails sortants) qui peut être utilisé par les routeurs IPL.
Ce service permet aux routeurs IPL d'envoyer des mails sans configuration spécifique.

Cocher cette case pour envoyer des mails sans autre configuration du routeur; autrement, saisir le nom du serveur SMTP à utiliser ainsi que le N° de port

Remarque :
On peut souhaiter recevoir l'alarme sous forme d'**un message SMS** sur un mobile. Ceci est possible en adressant l'e-mail d'alarme vers une adresse mail ouverte chez l'opérateur de téléphonie mobile qui le route ensuite vers le portable associé. Les opérateurs de téléphonie mobile offrent cette fonction. On consultera notre service hotline pour la mise en œuvre.

1 Diagnostic visuel de défaut de fonctionnement

Après la mise sous tension, le voyant « Opération » s'éclaire en rouge durant 30 secondes environ pendant la phase d'initialisation du routeur
Après ce délai, le voyant passe au vert lorsque le produit est prêt à fonctionner.
Si le voyant reste éclairé rouge après de délai, le routeur est probablement en panne ; contacter la hotline.

2 Menu Diagnostic

2.1 Journaux

Pour accéder aux différents journaux,

- Sélectionner la page le menu Diagnostic >Journal

Journal principal
Le journal principal enregistre et horodate les principaux événements du routeur et en particulier :
Etat de la carte SIM
Connexions et déconnexions du réseau cellulaire
Connexions et déconnexions des VPN
Connexion / déconnexions d'utilisateurs distants
Initialisation et démarrage du routeur

Journal OpenVPN et journal IPSec
Ces journaux enregistrent en détail et horodatent les principaux événements relatifs aux connexions et déconnexions VPN.

Journal avancé
Ce journal est destiné à notre hotline en cas d'événements particulièrement difficiles à analyser avec les autres outils.
Etat de l'interface cellulaire du routeur

- Sélectionner le menu Diagnostic > Etat réseau > Interfaces

Etat de l'interface cellulaire / Paramètres de base :

Champ « Connecté » : Oui / Non

Champ « Adresse IP » : Adresse IP attribué à l'interface cellulaire du routeur.

Champ « Qualité du signal » : Valeur en dBm du signal reçu
(voir tableau des valeurs requises au chapitre Installation)

Champ « Type de réseau » : Type du réseau cellulaire auquel le routeur s'est connecté (4G, 3G, GPRS)

Champ « Opérateur » : Type du réseau cellulaire auquel le routeur s'est connecté

Champ « Cell Id » : N° de la cellule sur laquelle le routeur est inscrit.

Champ « Débit montant maximal» et « Débit descendant maximal» :
Débit maximal possible

2.2 Etat des passerelles série

- Sélectionner le menu Diagnostic > Etat des passerelles

Cette page permet d'afficher l'état courant du paramétrage des passerelles, le nombre d'octets et de trames échangées et le nombre de trames en erreur.

Le menu « Visualisation des données série » permet de visualiser le trafic RX et TX sur la liaison série.

2.3 Outils « Ping »

Cette page permet de commander l'émission d'une trame « ping » vers une machine du réseau raccordé au routeur.

2.4 Outil « Scanner WiFi »

Le scanner WiFi affiche la liste des réseaux WiFi détectés par le routeur.

Pour chacun de réseaux détectés, le scanner affiche les informations suivantes :
Identificateur du réseau (SSID)
L'adresse MAC du point d'accès
N° du canal
Niveau de réception

Le scanner est utile afin de choisir un N° de canal non utilisé lorsque l'on souhaite configurer le canal en point d'accès.

Réciproquement, il facilite la configuration de l'interface WiFi du routeur lorsque l'interface WiFi doit être utilisée en client.

Remarque : le scanner Wifi ne peut fonctionner que si l'interface WiFi est déclarée comme client WiFi (et pas comme point d'accès WiFi).

Pour déclarer l'Interface WiFi comme client WiFi afin d'utiliser le Scanner :

- Dans le menu Configuration > WAN, sélectionner WiFi dans la liste.
- Dans le menu Configuration > LAN > Point d'accès WiFi, décocher la case « Activer le point d'accès WiFi ».

3 Sauvegarde et chargement d'un fichier de paramètres

Une fois un produit configuré, il est possible d'enregistrer la configuration dans la mémoire du routeur, ou de la sauvegarder sous forme d'un fichier éditable.

Réciproquement, il est possible de charger une configuration parmi l'ensemble des configurations enregistrées dans la mémoire du produit ou bien de restaurer un fichier de configuration sauvegardé dans un PC.

- Sélectionner les menus Maintenance > Gestion des configurations.

Le tableau qui enregistre la liste des configurations enregistrées dans la mémoire du routeur s'affiche.

Pour enregistrer la configuration courante dans la mémoire du routeur,

- Face au champ « Nom de la configuration », attribuer un nom pour la configuration et cliquer le bouton « Save ».

La configuration s'ajoute à la liste dans le tableau des « configurations sauvegardées ».

Pour charger comme configuration courante l'une des configurations de la liste,

- sélectionner la configuration dans la liste et cliquer charger.

Pour sauvegarder la configuration courante dans un fichier .txt,

- commencer par enregistrer la configuration courante dans la mémoire du routeur comme indiqué précédemment,
- puis sélectionner dans la liste la configuration à exporter et cliquer le bouton « Exporter vers le PC ».

Pour restaurer un fichier de paramètres sauvegardé,

• Cliquer le bouton « choisissez un fichier» puis sélectionner le fichier (XXX.txt) à restituer.

• Modifier éventuellement le nom du fichier et cliquer le bouton « Importer ». la configuration correspondante apparaît dans la liste « Configurations sauvegardées».

• Sélectionner la configuration dans la liste puis cliquer « Charger » ; elle remplace la configuration courante.

Note : Un fichier de configuration ne peut être restauré que s'il a été constitué avec la même version de firmware.

4 Mise à jour du firmware

Elle s’effectue par la prise Ethernet ou bien à distance.

Après la mise à jour, le produit utilise le fichier de paramétrage initialement enregistré.

Si la mise à jour est effectuée à distance, on vérifiera que la nouvelle version de firmware peut utiliser le fichier initial.

Pour effectuer la mise à jour du logiciel,

• sélectionner les menus Maintenance > Mise à jour du logiciel ;
• sélectionner le fichier du nouveau firmware ;
• Cliquer le bouton « Mettre à jour maintenant »

M2Me_Connect pour la prise en main de machine à distance

Le service M2e_Connect est une option du routeur IPL qu'il faut commander séparément.

Référence de l'option : M2Me_pack_initial

1 Présentation

Principe
Il arrive fréquemment que la connexion entre le PC et le routeur sur l'Internet ne soit pas possible parce que ni le PC ni le routeur ne disposent d'adresses IP publiques, ou bien faute de pouvoir régler le routeur d'entreprise ou bien faute d'autorisation.

Le service M2Me_Connect permet de résoudre la difficulté : Grâce à M2Me_Connect, le PC se connecte à la machine, pour une opération de maintenance par exemple, même si , ni le PC ni le routeur ne possèdent d'adresse publique.

Fonctionnement
L'utilisateur du PC enregistre dans son logiciel M2Me_Secure le nom du certificat d'authentification du routeur IPL.

Lorsque l'utilisateur ouvre son logiciel M2Me_Secure, son PC établit automatiquement une connexion sécurisée vers le service M2Me_Connect. Il s'authentifie sur le service.

De son côté, le routeur fait de même dès qu'il est sous tension.

Une fois connectés au service, et après authentification réciproque, le PC et le routeur établissent un VPN de bout en bout.

2 Paramétrage d'une connexion au service M2Me_Connect

Pour paramétrer la connexion au service M2Me_Connect, il suffit de paramétrer le VPN établi depuis le routeur vers le service M2Me_Connect ainsi que le VPN établi depuis le PC vers le service M2Me_Connect.

Chacun de ces VPN peut être supporté soit par le protocole UDP soit par le protocole TCP.

L'utilisation du protocole UDP plutôt que TCP est recommandée.

Etape 1 : Paramétrage du routeur

- Sélectionner le menu Configuration > Accès distant > M2Me_Connect

Paramètre « Activer » :
Cocher la case pour activer la connexion au service M2Me_Connect.

Paramètres « Port TCP et paramètres « Port UDP » :
Cocher tous les ports UDP ou TCP que le routeur peut tester afin de tenter d'établir la connexion vers le service M2Me_Connect.

Si un port UDP ou TCP unique a été autorisé, cocher la case correspondante ou bien saisir la valeur de ce N° de port TCP ou UDP.

Note : L'utilisation du protocole UDP est préférable à TCP.

- Si un serveur proxy filtre les connexions sortantes, décocher la case « Accès à Internet (pas de proxy » et saisir les paramètres de ce serveur :

Paramètre « Serveur proxy » :
Type (http ou SOCKS5),
Adresses et N° de port,
Authentification Login et mot de passe à fournir pour s'y présenter (éventuellement).

Attention : « La clé de produit » que l'on trouve dans le menu « A propos » doit être copiée afin d'être reporté dans le logiciel M2Medu PC de télémaintenance. C'est en effet cette clé qui autorise l'accès à la machine.

- Tester la connexion

Pour commander la connexion du routeur au service M2Me_Connect, cliquer le bouton « Connecter maintenant ».
Pour vérifier que la connexion s'effectue normalement, sélectionner le menu « Diagnostic » puis « Etat réseau » puis « M2Me ».
Lorsque la connexion aboutit, le message « Connecté » s'affiche dans le champ « Etat » ainsi que le N° de port et le protocole utilisé.

Etape 2 : Paramétrage du logiciel M2Me_Secure du PC distant

- Ouvrir le logiciel M2Me_Secure et saisir l'identificateur et le mot de passe de l'utilisateur (c'est celui qui sera ensuite contrôlé par le routeur pour identifier l'utilisateur du PC).
- Pour créer la connexion avec le site du routeur, cliquer l'icône « Menu » puis « Nouveau site ».
- Sélectionner l'onglet « Général », et saisir le nom du site du routeur (ce libellé n'a qu'un rôle mnémonique).
- Sélectionner l'onglet « Connexion » ; cocher les cases « Ce site est accessible par Internet » et « Ce site est visible à travers le service M2Me ».

- Saisir le code appelé « Product key » ; on le trouve dans le menu « A propos » du routeur.
  Il s'agit du résumé du certificat d'authentification enregistré dans le routeur en usine; il permet au PC de s'adresser au routeur lorsque l'un et l'autre sont connectés au service M2Me_Connect.

Le mot de passe doit être gardé secret par chaque utilisateur ; il n'apparaît jamais en clair.

Paramètre « e-mail » :

Il sera utilisé par le routeur soit pour transmettre un e-mail d'alarme à la suite du passage en défaut de l'entrée TOR, soit lorsque l'utilisateur souhaite se connecter par l'Internet ; dans ce cas, l'adresse IP publique du routeur peut lui être transmise par e-mail.

Paramètre « Filtre pare-feu » :

Un filtre est un ensemble de règles de sécurité limitant l'accès aux machines et services raccordées derrière le routeur. Un filtre peut être appliqué pour un ou plusieurs utilisateurs ce qui permet de différencier les droits d'accès aux machines en fonction de qui se connecte. Par défaut, rien n'est filtré.

Paramètre »Certificat » :

Ce paramètre n'apparaît que si l'on a choisi un VPN L2TP/IPSec ou TLS/SSL avec authentification par Certificat numérique. Il décrit les champs du certificat qui doivent être contrôlés par le routeur.

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 191 (0xbf)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=FR, ST=Isere, L=Meylan, O=ETIC Telecommunications, OU=Security,
CN=ETIC_Telecom_CA/emailAddress=Security@etictelecom.com
    Validity
      Not Before: Nov 22 14:46:58 2007 GMT
      Not After : Nov 14 14:46:58 2037 GMT
    Subject: C=FR, ST=Isere, L=Meylan, O=ETIC Telecommunications, OU=Security, CN=b4b4d3c9-b200-4869-8637-
edb3d421d55a/emailAddress=b4b4d3c9-b200-4869-8637-edb3d421d55a@etictelecom.com
    Subject Public Key Info:
```

ETIC TELECOM
13 chemin du vieux Chêne
38240 Meylan
France
contact@etictelecom.com